Faculdade de Engenharia da Universidade do Porto

Segurança na Circulação de Informação Clínica

Sara Campos Araújo

Licenciada em Engenharia Electrónica e Informática pela

Universidade Lusíada

Dissertação submetida para satisfação parcial dos

requisitos do grau de

Mestre em Redes e Serviços de Comunicação

Dissertação realizada sob a supervisão de

Professor Doutor João Carlos Pascoal de Faria,

e co-orientação de Professor Doutor José Manuel de Magalhães Cruz

do Departamento de Engenharia Electrotécnica e de Computadores

da Faculdade de Engenharia da Universidade do Porto

Porto, Março de 2007

Informática ao Serviço da Medicina

«É como extrair ordem do caos tirando o proveito máximo da nossa imaginação e dos nossos talentos. Vamos, por exemplo, a um hospital, e vemos duplicações de trabalhos, erros humanos, desperdícios de tempo que pode custar vidas, diagnósticos honestos, mas incorrectos, que uma máquina pode corrigir numa questão de segundos, Médicos cheios de trabalho a consultar fichas quando podiam estar a aliviar sofrimento... e, num instante, instalamos um sistema e temos o prazer de ver tudo encaixar no seu lugar, tudo funcionar, e sabemos que foi obra nossa. (...)
Pelo mais simples dos métodos, libertamos pobres escriturários atormentados de milhares de horas de enfado. (...) torna a humanidade mais humana e não menos.»

Irwin Shaw, in "Bread upon the waters", 1981

RESUMO

Com vista à melhoria dos cuidados de saúde prestados ao cidadão, assiste-se em Portugal ao crescente registo e circulação de informação clínica em formato electrónico. Este facto traz consigo também preocupações acrescidas com a segurança e privacidade da informação clínica e dos sistemas de informação clínica.

Nesta dissertação, após um levantamento das questões de segurança a considerar nos sistemas de informação clínica, são apresentados os resultados de uma análise efectuada ao estado actual da segurança dos sistemas de informação clínica em Portugal no que se refere ao acesso, armazenamento e circulação da informação clínica do paciente. Esta análise incidiu sobre as infra-estruturas e as aplicações informáticas das unidades de saúde do Sistema Nacional de Saúde (SNS), com especial foco no ambiente de utilização do processo clínico electrónico. As aplicações analisadas foram o SONHO, o SINUS e os módulos de apoio ao médico (SAM) e às práticas de enfermagem (SAPE).

São também analisadas, na óptica da segurança, algumas tendências de evolução dos sistemas de informação clínica tirando partido de tecnologias emergentes.

No sentido de reforçar a segurança da informação clínica e ultrapassar as muitas deficiências encontradas actualmente, propõe-se um conjunto de medidas que incluem a implementação de uma Política de Segurança Informática para o SNS e a implementação de uma infra-estrutura de chaves públicas (PKI) para a Rede Informática da Saúde (RIS). Estas medidas são convenientemente justificadas e, em termos gerais, delineadas.

Palavras-chave: Segurança, Sistemas de Informação na Saúde, Normas, Infra-estrutura de Chaves Públicas (PKI)

ABSTRACT

In order to improve the health care services provided to the citizens, there is an increasing registration and circulation of clinical information in electronic format in Portugal. This tendency is accompanied by increasing concerns with the security and privacy of the clinical information.

In this dissertation, after analyzing the key security issues of the clinical information systems, we present the results of an analysis performed to asses the current security status of the Clinical Information Systems in Portugal as for access, storage and circulation of the patient's clinical information. This analysis was carried through in the contexts of network infrastructures and clinical applications for the health care units of the National Health System (SNS), with special focus for the electronic clinical process. The clinical application analysed were SONHO, SINUS, a module to support the doctors' activities (SAM) and nursing practices (SAPE).

An approach is also made to the Systems Information and Communication trends, due to emerging technologies and to the new security problems that arise.

In order to improve the security of the clinical information and overcome the many deficiencies found presently, it is proposed a set of measures, comprising the proposal for the implementation of an Informatics Security Policy for the SNS and the implementation of a public key infrastructure (PKI) for the Health Informatics Network (RIS), that as conveniently justified and generally delineated.

Keywords: Security, Healthcare Information Systems, Standards, Public Key Infrastructure (PKI)

AGRADECIMENTOS

No finalizar deste trabalho, quero expressar meus agradecimentos a todas as pessoas que, directa ou indirectamente, contribuíram para a sua concretização. Pela razão de que muitas pessoas colaboraram, citar nomes seria algo difícil de ser feito sem cometer a injustiça da omissão.

Em particular gostaria de referir o apoio dos orientadores desta dissertação, o Professor Doutor João Pascoal Faria e o Professor Doutor José Manuel de Magalhães Cruz.

Em especial, desejo agradecer à minha família, ao meu marido Paulo, pela paciência e incentivos nos momentos de desânimo e ao meu pequenote João Pedro que nasceu durante esta jornada, pelas gargalhadas e brincadeiras nos momentos de descontracção.

A todos o meu muito obrigado.

E a Deus, pela vida e pelas oportunidades nela surgidas.

INDICE

INDICE DE FIGURAS

INDICE DE TABELAS

LISTA DE ABREVIATURAS

AES – Advanced Encryption Standard

ARP – Address Resolution Protocol

ATM – Asynchronous Transfer Mode

CIPE – Classificação Internacional para a Prática de Enfermagem

CNPD – Comissão Nacional Protecção de Dados.

DHCP – Domain Host Control Protocol.

DICOM – Digital Imaging and Communications in Medicine.

DMZ – DeMilitarized Zone.

DNS – Domain Name System.

DoS – Denial of Service.

ECEE – Entidade Certificadora Electrónica do Estado

EU – União Europeia

FTP – File Transfer Protocol

GDH – Grupo de Diagnóstico Homogéneos

HIPAA – Health Insurance Portability Accountability Act

HL7 – Health Level Seven

ICD – International Classification of Disease

IDS – Intrusion Detection System

IEEE – Institute of Electrical and Electronics Engineers

IGIF – Instituto de Gestão Informática e Financeira da Saúde

IMAPS – Interactive Mail Access Protocol Secure

IP – Internet Protocol

IPsec – IP Security

LDAP – Lightweight Directory Access Protocol

MAC – Media Access Control

MIME – Multipurpose Internet Mail Extension

MPLS – Multiprotocol Label Switching

MS – Ministério da Saúde

PACS – Picture Archive and Communication System

PAM – Pluggable Authentication Module

PCE – Processo Clínico Electrónico

PDA – Personal Digital Assistance

PEM – Privacy Enhanced Mail

PGP – Pretty Good Privacy

PKI – Public Key Infrastructure

POP – Post Office Protocol

POPS – Post Office Protocol Secure

RDIS – Rede Digital com Integração de Serviços

RIS – Rede Informática da Saúde

RPC – Remote Procedure Call

S/HTTP – Secure Hyper Text Transfer Protocol

S/MIME – Secure Multipurpose Internet Mail Extensions

SAM – Sistema de Apoio ao Médico

SAPE – Sistema de Apoio à Prática de Enfermagem

SET – Secure Electronic Transactions

SGBD – Sistema de Gestão de Base de Dados

SHTTP – Secure HyperText Transfer Protocol

SINUS – Sistema de Informação para Unidades de Saúde

SMTP – Simple Mail Transfer Protocol

SMTPS – Simple Mail Transfer Protocol Secure

SNOMED – Standard Nomenclature of Medicine

SNS – Sistema Nacional de Saúde

SONHO – Sistema Integrado de Informação Hospitalar

SSH – Secure SHell

SSL – Secure Socket Layer

TCP/IP – Transmission Control Protocol / Internet Protocol

TELNET – Terminal emulation program for TCP/IP network

TLS – Transport Layer Security

UMLS – Unified Medical Language System

VLANs – Virtual Local Area Network

VPN – Virtual Private Network

XML – Extensible Markup Language

1 INTRODUÇÃO

Na Saúde, diversas iniciativas nacionais e internacionais tiveram como objectivo a promoção e efectivação da utilização de serviços electrónicos, recorrendo às novas tecnologias de informação, ao audiovisual e às comunicações (nomeadamente, via Internet), originando o que globalmente se designa por eSaúde (Figura 1 e Figura 2), para a qual contribui o decréscimo nos custos de armazenamento digital e transmissão de dados. A eSaúde visa a exploração da informação e a comunicação, nomeadamente via Internet, para melhorar a prestação de cuidados de saúde, de disseminação de informação e até a aquisição de bens e serviços, com valor acrescentado.

Figura 1 – Representação Física da eSaúde

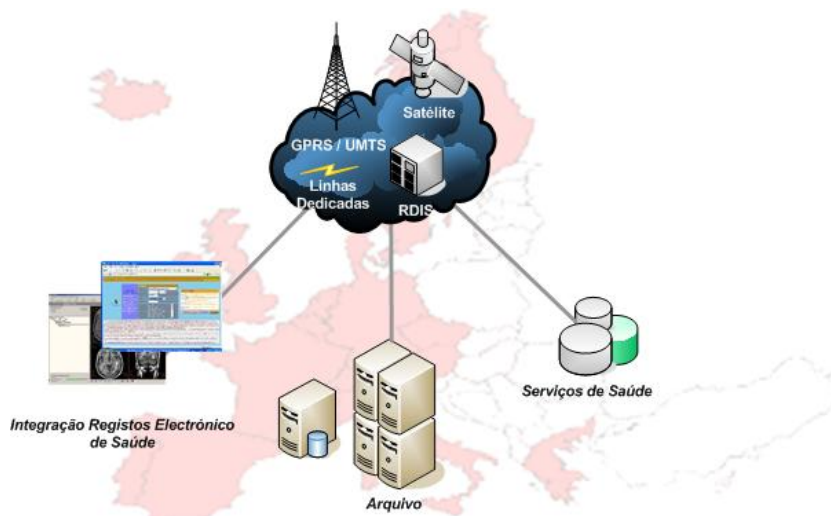



Figura 2 – Representação Lógica da eSaúde

A União Europeia promoveu a iniciativa eEurope 2002, visando desenvolver a economia digital e providenciar aos cidadãos Europeus os benefícios da utilização da Internet. No que respeita à Saúde, destacam-se quatro linhas de orientação desta iniciativa: garantir a existência de infra-estruturas telemáticas, incluindo redes regionais para os prestadores de cuidados de saúde; identificar e difundir as melhores práticas de saúde on-line e estabelecer critérios para avaliação de desempenho; estabelecer critérios de qualidade para os portais da saúde; criar redes de tecnologias e avaliação de dados no domínio da saúde.

Mais recentemente, o plano eEurope 2005 [1] estimula serviços, aplicações e conteúdos que criem novos mercados, reduzam custos e incrementem a produtividade em toda a economia, destacando-se pelo âmbito deste estudo a promoção de serviços electrónicos de saúde, o eSaúde. Para a prossecução deste fim foram propostas três acções: utilização de cartões de saúde electrónicos; expansão de redes de informação de saúde; estabelecimento de serviços de saúde *on-line*.

O sector da saúde em Portugal não ficou de facto à margem deste processo de mudança e por isso a telemática aplicada à saúde tem vindo progressivamente a afirmar-se como uma resposta às inúmeras necessidades com que o sistema de saúde se confronta.

Assim, os efeitos da telemática aplicada à saúde têm sido largamente debatidos, não deixando de parte aspectos éticos e legais, nomeadamente no que se refere à privacidade, confidencialidade, direitos de acesso e de propriedade, protecção e segurança dos dados, fiabilidade dos produtos e regulamentação da prática profissional em Portugal e no mundo.

1.1. Enquadramento

O registo electrónico dos dados clínicos dos pacientes e a sua partilha entre todos os profissionais envolvidos é fundamental para optimizar os processos de prestação de cuidados de saúde. Para que o registo e circulação da informação clínica em formato electrónico seja bem aceite, é fundamental assegurar que este tipo de circulação é fiável e seguro. É importante conseguir um bom compromisso entre dois objectivos que por vezes entram em conflito: melhorar os cuidados de saúde prestados ao cidadão e garantir a sua privacidade.

A Figura 3 pretende definir o modelo que irá servir de base à análise desta problemática de segurança.

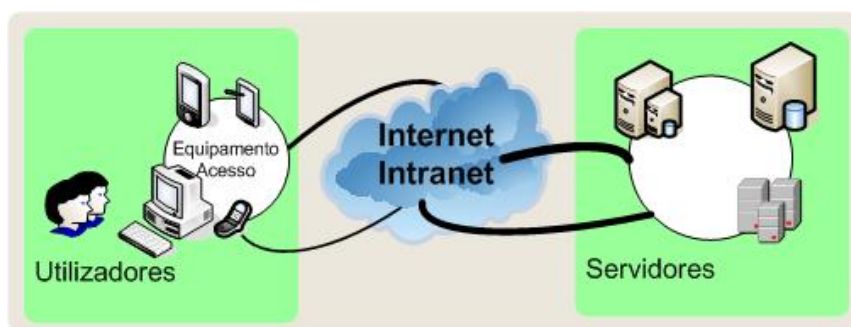



Figura 3 – Modelo de Segurança dos Sistemas de Informação Clínica.

As questões foco de atenção desta análise são: o desenvolvimento ou implementação dos sistemas de informação clínica; o controlo de acessos à informação clínica; o armazenamento da informação clínica; a circulação da informação clínica; normas e princípios ético-legais.

Para cada um destes pontos serão detalhados alguns aspectos importantes relacionados com as ameaças à segurança as vulnerabilidades dos sistemas de informação clínica e serão também propostas soluções e mecanismos de segurança a usar.

1.2. Objectivos

O tema foco desta tese tem sido alvo de largas discussões nos meios relacionados com a segurança na área da saúde. Os principais objectivos em análise são:

- Estudar do estado da arte da segurança dos sistemas de informação clínica em Portugal.
- Estudar a situação actual e as necessidades futuras relativas à circulação da informação clínica no contexto da Telemedicina, *e*Saúde, acesso ao processo clínico electrónico, novos canais de comunicação e informação clínica na posse do utente.
- Propor medidas, tecnológicas ou outras, para melhorar a segurança na circulação de informação clínica e na utilização da informática nas instituições de saúde pública em geral.

1.3. Motivação

A razão que levou à selecção deste tema foi o facto de ser actual e estar a causar uma preocupação crescente aos profissionais envolvidos e aos cidadãos (por exemplo, perigo de divulgação de informação privada do paciente). Esta escolha deve-se também ao facto de a autora estar envolvida profissionalmente nestas questões, pelo seu cargo de técnica de informática numa instituição de saúde.

1.4. Organização do Documento

Esta dissertação encontra-se dividida em seis partes: o actual capítulo 1 introduz o contexto e as motivações do trabalho. No Capítulo 2 são globalmente apresentados os aspectos críticos na segurança do registo clínico electrónico do ponto de vista do desenvolvimento ou implementação do sistema de registo, do ponto de vista do controlo de acessos, das comunicações, e das questões ético-legais, normas e recomendações actuais. No Capítulo 3 realiza-se uma análise global do estado actual da segurança das infra-estruturas e dos principais sistemas de informação clínicos em Portugal no SNS, no que se refere aos pontos anteriormente apontados. No Capítulo 4 são apresentadas as tendências e as tecnologias emergentes no domínio dos sistemas de informação clínica na área médica. No Capítulo 5 sugere-se um conjunto de medidas com vista ao reforço da segurança no acesso, armazenamento e circulação da informação clínica do paciente. Entre outras medidas, é proposta a implementação de uma Política de Segurança Informática para o Ministério da Saúde e a implementação de uma infra-estrutura de chaves públicas (PKI) para a Rede Informática da Saúde (RIS) em Portugal. No último capítulo, apresentam-se as conclusões tiradas a partir do estudo realizado.

2 QUESTÕES CHAVE NA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO CLÍNICA

2.1. Introdução

Neste capítulo irá ser identificado e analisado um conjunto de aspectos críticos na segurança dos dados clínicos electrónicos do paciente, que irão servir de base ao estudo de um caso no Capítulo 3. Para além disto, para as ameaças e vulnerabilidades identificadas, serão apresentados mecanismos, serviços, políticas e dispositivos de segurança necessários para assegurar a segurança no acesso, armazenamento e circulação de informação clínica do paciente em formato electrónico.

A análise de segurança irá incidir nas principais áreas de preocupação dos sistemas de informação clínica como referido no Capítulo 1 (no ponto 1.1) [142]. No ponto desenvolvimento e implementação do sistema de informação para o registo clínico electrónico do paciente, serão tidos em consideração algumas questões como a arquitectura e a tecnologia das aplicações e base de dados. Questões de segurança relacionadas com os utilizadores (por exemplo a sua identificação), equipamento de acesso e aplicações serão consideradas na introdução e acesso à informação clínica do paciente. No que diz respeito ao armazenamento dessa informação a atenção está orientada para as bases de dados, os servidores e computadores clientes. Outro aspecto crítico no sistema de informação clínica é o das comunicações, as infra-estruturas e os serviços de rede que suportam a circulação da informação. Na base de toda esta estrutura estão questões e princípios ético-legais que suportam a actividade dos diferentes profissionais no processo de prestação de cuidados de saúde em Portugal. E, finalmente, serão referidas algumas normas internacionais que favorece a segurança e a interoperabilidade dos sistemas electrónicos clínicos à escala global.

Para além disto, o estudo abrange dois cenários: o acesso e manuseamento da informação na rede interna da instituição; o acesso à informação proveniente do exterior da instituição (acesso via intranet da saúde –RIS– ou num universo mais alargado da Internet). Destes cenários, o mais exigente em termos de segurança é o segundo. No entanto, ambos exigem cuidados que abrangem os seguintes aspectos: comunicações e privacidade; integridade dos dados; identificação e controlo de acesso dos utilizadores; monitorização e auditoria; segurança física e adesão a padrões de arquitectura aberta.

2.1.1. Registos Clínicos

O **registo clínico electrónico** é um conjunto de informação estruturada e codificada que contém dados relacionados com a saúde e a doença de um paciente. Por exemplo, estes registos contêm dados relativos à história clínica do paciente, diagnósticos, tratamentos efectuados, prescrições de meios complementares de diagnóstico e terapêutica, diário de consulta ou internamento, cirurgias e outros. Habitualmente, estes registos são feitos por médicos, enfermeiros, administrativos e outros profissionais de saúde. É com base nesta informação proveniente de diversas fontes e em diferentes formatos (por exemplo: texto, imagem e som) que é organizado o processo (ou registo) clínico electrónico do paciente. Ele vai permitir, de forma controlada, partilhar a informação entre diferentes profissionais de saúde intra ou inter instituições e disponibilizá-la por diferentes formas de visualização e análise.

O **processo clínico electrónico** é um sistema integrado e distribuído de informação clínica do paciente associado a um conjunto de aplicações que a manipulam. O conjunto dessas aplicações constituem os **sistemas de informação clínica** e permitem por exemplo, auxiliar na prestação de cuidados de saúde; auxiliar a decisão clínica; avaliar a qualidade dos cuidados prestados; auxiliar na gestão e planeamento dos cuidados de saúde; auxiliar na investigação; auxiliar na formação médica.

Em termos práticos, a distinção entre "sistema de informação clínica", "processo clínico electrónico" e "registo clínico electrónico" é diminuta, pelo que todos eles serão usados de uma forma indiferenciada daqui para a frente.

2.1.2. Aspectos de Segurança

Os aspectos de segurança são essenciais e complementares aos sistemas de informação clínica, devendo a sua conjunção ser feita em função das necessidades específicas da rede, do sistema de informação ou do ambiente de que se trata.

A **confidencialidade** (privacidade ou sigilo) é a garantia de que os dados dos pacientes são protegidos e não são disponibilizados ou divulgados sem autorização prévia do paciente.

Os aspectos de **disponibilidade** garantem que, mesmo após a ocorrência de ataques à rede ou ao sistema informático, os recursos chave ficam disponíveis. Este aspecto é essencial em sistema de emergência ou cuidados intensivos.

Em muitos casos, mais importante do que garantir a confidencialidade da informação que está a ser veiculada ou armazenada é garantir que essa informação não é corrompida. Os aspectos de **integridade** abordam este tipo de problemática da segurança dos registos do paciente.

Outras propriedades como a legitimidade e autenticidade estão a tomar importância relevante na medida em que aumenta a transacção de informação por todo o mundo. Em muitas destas interacções, há que previamente garantir que as entidades intervenientes são quem afirmam ser, e é de extrema importância que uma entidade envolvida numa transacção não possa negar a sua participação nesse evento (garantia de não repúdio).

São consideradas ameaças à segurança dos registos clínicos, as ameaças a qualquer uma das três características essenciais anteriormente referidas.

Ameaças à confidencialidade ocorrem quando dados protegidos correm o risco de serem divulgados e passar por mãos não autorizadas, quer seja por forma acidental quer propositada. Por exemplo: acessos não autorizados aos registos do paciente; vulnerabilidades derivadas de partilha de senhas; intercepção não autorizada da informação que transita na rede; gestão não controlada da informação.

Ameaças à disponibilidade dos dados ou às funcionalidades do sistema ocorrem quando, por algum motivo, o sistema não tem meios de manter a funcionar de forma acessível serviços no momento que lhe são solicitados. Alguns exemplos de problemas poderão ser: falhas nos equipamentos ou serviços de rede (por exemplo: provocados pela falha de energia); erros no manuseamento do sistema; ataques intencionais para impedir o normal funcionamento do sistema; causas naturais (por exemplo: incêndios ou inundações); recursos insuficientes para o correcto funcionamento do sistema.

Ameaças à integridade ocorrem quando há risco de propositada ou acidentalmente, os conteúdos dos dados armazenados ou transmitidos ficarem inconsistentes ou corrompidos. As razões que poderão estar na origem das ameaças são, por exemplo, erros operacionais (na introdução e manipulação de dados); erros no *software*; vírus; mau funcionamento do equipamento.

2.2. Desenvolvimento e Implementação

A primeira coisa a pensar no desenvolvimento ou implementação de um sistema para registo clínico electrónico é nos propósitos a que se destina. É fundamental saber o que é que o sistema vai fazer, quais os seus principais objectivos e também a que utilizadores se destina. De seguida, definir as funcionalidades que deverá conter e o ambiente em que irá ser usado para que a escolha das tecnologias de implementação seja adequada.

No desenvolvimento do sistema de registo clínico electrónico, dever-se-á ainda ter em consideração os diferentes tipos de profissionais que irão estar envolvidos: pessoal de enfermagem, médicos, administrativos e informáticos são alguns deles. Deverão ser reunidos esforços no sentido

de obter usabilidade e ao memo tempo segurança do sistema. Pensando desta forma desde o início, a construção do sistema será mais estruturada e estará mais adaptada aos utilizadores e aos propósitos para a qual foi definido, e resultando num sistema mais seguro.

A integração com outros módulos que constitui o sistema deverá ser fácil e não interferir com as suas funcionalidades, mas tudo deverá funcionar com requisitos de segurança.

2.2.1. Ameaças à Segurança e Vulnerabilidades

A estrutura heterogénea dos sistemas de registo clínico electrónico faz com que seja necessário um elevado nível de protecção e segurança devido à sensibilidade da informação pessoal e clínica.

As preocupações de segurança derivam do facto de diferentes fontes terem requisitos tecnológicos diferentes e políticas estabelecidas também diferentes, e do resultado da sua integração poder não ser o esperado. As instituições podem partilhar informação relevante entre si, confiando mutuamente que a informação irá ser mantida confidencial e que será apenas usada para o propósito definido. Neste caso, a linha entre utilizadores internos e externos da rede não está muito bem definida. Pessoas de diferentes organizações podem aceder à informação de muitas outras redes e torna-se difícil gerir e auditar quem tem acesso a que informação e que mecanismos de segurança deverá ter todo o sistema.

Por outro lado, como os diferentes módulos têm de ser capazes de interoperar diferentes tecnologias, vulnerabilidades que poderiam ser controladas individualmente poderão ter comportamentos inesperados quando interligados.

Outra questão importante, é o uso da linguagem e vocabulário quando se está a desenvolver as interfaces do utilizador. Se as regras não forem consideradas, informação ambígua e redundante poderá ser inserida e mantida o que irá afectar enormemente a eficácia e celeridade do processo de acesso e gestão da informação clínica. Para alem disto, o uso heterogéneo da informação tornará mais difícil a integração de todas as partes que constituem o sistema de registo clínico.

2.2.2. Soluções e Mecanismos de Segurança

O uso de estruturas de dados comuns e protocolos de comunicação permitem a interoperabilidade e troca de dados entre diferentes sistemas, por exemplo, em franca expansão a nível europeu o uso da norma HL7 (ver Anexo A). Neste contexto, é de salientar outras normas: a norma CR 13694 – “Safety and Security Related Software Quality Standards for Healthcare (SSQS)” focaliza a sua atenção na segurança do software, confidencialidade e integridade; ISO/TS

18308 – “Requirements for an Electronic Health Record Architecture” cujo o objectivo é fixar os requisitos clínicos e técnicos para uma arquitectura de registos electrónicos de saúde, que suporte o uso, a partilha e intercâmbio dos registos clínicos electrónicos entre diferentes sectores relacionados com os cuidados de saúde, diferentes países, e diferentes modelos transferência de informação clínica.

A normalização da informação de cuidados de saúde, também é muito importante na implementação de sistemas para registo clínico electrónico. A normalização fornece um conjunto de linhas de orientação que permitem que o sistema seja estruturado, aceite, mais fácil de compreender e usar. Para além disto pode evitar a fragmentação e redundância de dados e fornecer melhor qualidade dos sistemas de informação de saúde com recursos mínimos e custos baixos.

Em Portugal, no que se refere à classificação e codificação da informação clínica, são de realçar: o ICD-9[1] usado com vista a classificar e codificar informações médicas; o GDH[2] usado com intuito de classificar episódios de internamento de acordo com o ICD-9; o SNOMED[3] usado para descrever o resultado de testes patológicos; a CIPE[4] que é uma linguagem classificada que permite a produção de informação acerca das decisões e dos resultados da prática de enfermagem.

Outro aspecto a ter em consideração é que ao adoptar normalização internacional similar para sistemas de registo clínico electrónico, poderá ser possível atravessar fronteiras e procurar melhor tratamento noutros países na condição de que a informação possa estar disponível internacionalmente. Também permitiria mais um passo na investigação uma vez que esta poderia ser feita em diferentes partes do mundo.

2.3. Identificação e Autenticação

Num sistema seguro terão de existir meios para identificar os seus utilizadores, não apenas porque a sua identidade é essencial para decidir que tipo de acesso à informação deverão ter, mas também para ser possível rastrear as suas acções dentro do sistema. Por vezes, designa-se por autenticação à operação de identificação bem sucedida de um utilizado. Nesse sentido, de uma

---

[1] ICD - International Classification of Disease. Padrão criado com o objective de codificar e classificar informações médicas (ver, Anexo A).

[2] GDH - Grupo de Diagnóstico Homogéneos. Sistema de classificação de episódios de internamento (ver, Anexo A).

[3] SNOMED - Standard Nomenclature of Medicine. É uma nomenclatura criada para indexar um conjunto de registos médicos, incluindo sinais, sintomas, diagnósticos e procedimentos (ver, Anexo A).

[4] CIPE - Classificação Internacional para a Prática de Enfermagem (ver, Anexo A).

forma mais simples, num primeiro passo, o utilizador afirma ter uma certa identidade e no segundo passo do processo ele prova quem afirma ser, de uma maneira controlada pelo sistema.

Num sistema informático de registos clínicos, os utilizadores têm diferentes tarefas atribuídas e diferentes direitos de acesso à informação, pelo que deverão ser disponibilizadas diferentes formas de identificação e validação de um utilizador para que a privacidade e confiança possa ser assegurada. Este processo pode ser feito usando um dispositivo físico, como um testemunho (em inglês, token[5]) ou apresentando algo conhecido tal como uma senha ou "frase-senha" ou usando características biométricas. Estas são normalmente conhecidas como: *algo que o utilizador sabe* (por exemplo, uma senha); *algo que o utilizador tem* (por exemplo, dispositivos como *token*, cartão inteligente, etc.); *algo que o utilizador é* (leitura da íris, linhas das mãos). Para disponibilizar uma autenticação mais segura duas ou mais destas técnicas deverão ser usadas num só momento dependendo também do grau de segurança exigido pelo sistema.

2.3.1. Ameaças à Segurança e Vulnerabilidades

A forma mais comum de executar o processo de identificação e validação de um utilizador, referido anteriormente como "algo que o utilizador sabe", é exigir identificação nome-utilizador (identificação) e senha (autenticação) para permitir o acesso. Este método é fácil implementar e pode fornecer níveis de acesso à informação que compõe os registos clínicos.

Uma das ameaças mais importantes que este tipo de sistema enfrenta é a chamada "engenharia social". Este tipo de ameaça é bastante fácil de concretizar e por vezes dá ao atacante tudo o que ele precisa de saber sem muito trabalho. Uma forma habitual de acção é um atacante fingir ser um administrador de rede telefonando a uma pessoa menos informada exigindo nome-utilizador / senha para solucionar um suposto problema. Isto pode parecer simples mas pode ser muito eficaz. Hoje em dia, num ambiente de prestação de cuidados de saúde, grande parte dos utilizadores não tem conhecimentos para solucionar questões técnicas, por isso facilmente fornecem a informação exigida sem sequer pensar duas vezes.

No que diz respeito às senhas, existem alguns problemas de segurança que não são fáceis de evitar ou resolver. O principal problema é a escolha de senhas fracas, podendo facilmente ser obtidas através de ataques de dicionário ou de força bruta. Por outro lado, se as senhas são demasiadas complexas as pessoas normalmente esquecem-nas e tendem a escrevê-las em papel deixando-as acessíveis junto ao seu posto de trabalho. Frequentemente, nos sistemas de registo

[5] token – Dispositivo físico ou um testemunho, geralmente ligado à porta USB do computador, que armazena as chaves privadas e os certificados digitais, e restante identificação do utilizador, permitindo a sua validação pelo sistema.

clínico electrónico, os utilizadores necessitam de aceder a diferentes tipos de informação várias vezes ao dia. Se as senhas são simples, os utilizadores tem a sua tarefa facilitada, mas isto é um considerável risco de segurança. Se são muito complexas ou alteradas frequentemente, os utilizadores têm que ter outros meios de memorização para que possam usar o sistema. A usabilidade e disponibilidade são fundamentais nos sistemas de registo clínico electrónico.

Outro problema é o facto de os médicos frequentemente passarem as suas senhas a outros profissionais, tais como secretárias ou pessoal de enfermagem. Isto ainda é pior porque uma vez dada a senha já não a podemos controlar.

Outros problemas técnicos ainda mais complicados podem surgir. Por exemplo, se as senhas são armazenadas em claro, qualquer pessoa com acesso ao ficheiro de senhas ou escutando ilicitamente a rede pode obtê-las. Mais ainda, os atacantes possuem ferramentas que lhes permitem obter e decifrar senhas cifradas.

Estes são alguns dos mais pertinentes problemas de segurança que este tipo de identificação e autenticação têm. No entanto, existem formas para controlar e estabelecer alguns obstáculos para evitá-los, que serão mencionados posteriormente.

O processo de identificação e autenticação conhecido por "algo que o utilizador possui" utiliza um *token*, cartão inteligente ou qualquer outro objecto que contenha alguma informação usada durante a autenticação. Normalmente estão alojados em sistemas que exigem uma autenticação complementar. Nos sistemas de registo clínico electrónico podem ser usados quando se acede a máquinas específicas que contenham informação de pacientes altamente protegida (por exemplo, cancro ou SIDA). Algumas questões de segurança devem ser consideradas, pois um objecto como um *token* pode ser perdido ou até roubado e com ele toda a informação nele contida. Se esse objecto for cedido a um terceira pessoa, poderá pôr em risco a confidencialidade desses registos.

O processo de identificação e autenticação conhecido por "algo que o utilizador é", também designado por biométrico, faz uso de algumas características humanas, universais e mensuráveis e com um certo grau de exactidão. Impressão digital, padrão da íris e geometria da mão são apenas algumas das características mais usadas pelo processo. Este tipo de métodos é usado principalmente para implementar segurança física, por exemplo no acesso a lugares reservados, tais como laboratórios de alta segurança (por exemplo, de doenças infecto-contagiosas), ou de investigação. Alguns dos problemas de segurança podem surgir da inexactidão do sistema. Erro por aceitar utilizadores não autorizados ou negar acesso a utilizadores autorizados pode ser um problema, respectivamente, de confidencialidade e disponibilidade da informação.

Outro problema pode ser o caso do sistema ser incómodo e os utilizadores recusarem o seu uso e tentarem encontrar formas de contornar as medidas de segurança.

2.3.2. Soluções e Mecanismos de Segurança

Existem algumas recomendações a ter em consideração quando se identificam e autenticam utilizadores de sistemas de registo clínico electrónico. Certamente que não é possível aplicar controlos de segurança para enfrentar todas as ameaças identificadas anteriormente. Isto poderá ser verdade para as questões debatidas mas se algumas das acções e técnicas forem aplicadas, constituirão obstáculos e irão minimizar as consequências a futuros ataques à segurança.

No processo de identificação e autenticação referido por "algo que o utilizador sabe"**,** os utilizadores normalmente estão pouco preparados para utilizar computadores. Alguns deles ainda vêem estas máquinas como caixas negras mágicas. Sobretudo as pessoas precisão de saber como usá-los e como funcionam para que o seu trabalho possa ser feito de uma forma eficaz e segura. Formação e sensibilização são o primeiro passo para evitar alguns dos problemas de segurança no que concerne à identificação e autenticação dos utilizadores. Os utilizadores deverão ser capazes de saber a real importância das senhas e a que normas devem obedecer para que simples problemas de segurança possam ser evitados. Nunca deverão por exemplo dizer a outros as suas senhas porque na maior parte das vezes a mesma senha é usada para aceder a diferentes sistemas. Também a pessoa responsável por emitir e desactivar senhas deverá assegurar-se da identidade do utilizador com quem está a lidar.

A norma EN 12251 – "Secure User Identification for Healthcare – Management and security of authentication by passwords" (ver Anexo A), especifica um conjunto de requisitos orientados para a gestão e segurança da autenticação por senhas tendo por objectivo melhorar a autenticação individual dos utilizadores nos sistemas de registo clínico.

Para evitar a divulgação de senhas, estas devem ser mudadas regularmente; e para se evitar a sua divulgação devem ser suficientemente complexas para que os atacantes de dicionário (uso de palavras num dicionário para testar se existe correspondência) não sejam bem sucedidos. O tamanho e o formato deverão ser tidos em consideração e os utilizadores deverão ter conhecimento do tipo de senha que é permitida. Isto também pode ser feito ao nível da rede ao permitir aos utilizadores introduzir apenas um certo tipo de senhas. Também deve limitar-se as tentativas de conexão (login) para que o ataque por teclado não possa ser facilmente executado.

A auditoria é outra medida que pode não ser preventiva, mas pelo menos pode detectar a ocorrência de comportamentos estranhos e ser usada para evitar ataques futuros. É extremamente

importante o comportamento de um utilizador no sistema. A auditoria pode, por exemplo, detectar quando alguém está a tentar aceder à conta de outro utilizador ou detectar quando existem tentativas de ataque a ficheiros de senhas.

Os ficheiros de auditoria devem ser protegidos, i.é., não devem estar disponíveis para qualquer um, mas apenas para os utilizadores autorizados, e devem ser armazenados cifrados para que mesmo quando acedidos não seja fácil compreender o seu conteúdo.

No caso da identificação e autenticação referido por "algo que o utilizador possui", é relevante saber quem tem *token* ou cartão inteligente e quem os deve usar, mas o seu uso deve ser limitado apenas aos utilizadores autorizados. Os médicos das especialidades críticas devem tê-los para aceder aos sistemas. Quando se trata de casos de emergência, e se não for possível a presença do responsável, as acções deverão ser devidamente auditadas e documentadas para que o uso impróprio possa ser detectado e corrigido quando possível. O inventário deve ser mantido para ajudar na execução dessas acções.

Objectos roubados ou perdidos devem ser devidamente desactivados. Isto é mais fácil de executar se o inventário for mantido e actualizado correctamente.

Neste contexto a norma ENV 13729 – "Secure User Identification for Healthcare - Strong Authentication using Microprocessor Cards (SEC-ID/CARDS)" (ver Anexo A), está orientada para a identificação segura do utilizador nos sistemas de informação para a saúde. Preconiza autenticação forte através do uso de cartões profissionais de saúde e certificados digitais.

No processo de identificação e autenticação através de "algo que o utilizador é", o primeiro passo para os iniciar e usar apropriadamente é saber quando, onde e por quem estes sistemas biométricos vão ser utilizados. Devem ser escolhidos dependendo do nível de segurança exigido, quantos e que tipos de erros podem ser suportados e se o sistema tem o comportamento esperado. Se todos estes requisitos forem considerados, bem preparados, se os sistemas forem adequadamente testados e os utilizadores bem preparados para a sua utilização, podem ser evitados a maior parte dos problemas de segurança ligados ao acesso indevido.

2.4. Controlo de Acessos

O controlo de acessos é considerado o ponto central da segurança dos sistemas de informação. É um mecanismo usado para limitar as acções de utilizadores legítimos do sistema com base nas autorizações aplicáveis no momento do acesso. A autorização estabelece os direitos no

acesso ao sistema, isto é, estabelece o que é permitido ou não realizar no sistema. O seu principal objectivo é controlar o acesso dos seus principais intervenientes (utilizadores e processos) aos recursos do sistema (ficheiros, dispositivos periféricos, bases de dados, etc.). Geralmente obedecendo a certas restrições os utilizadores são identificados nos sistemas através de nomes curtos (por exemplo, primeiro e último nome, iniciais ou número mecanográfico do funcionário). Internamente, e por razões práticas, o sistema pode atribuir a cada utilizador um número único de identificação.

A identificação única dos processos (ou aplicações em execução) e das máquinas também não deve ser esquecido. A identificação das máquinas (habitualmente identificadas pelo seu nome ou endereço IP[6]) pode ser usado para permitir acessos de forma independente da identificação do utilizador por exemplo, definindo quais as máquinas que têm acesso a determinados serviços. Esta utilização, em complemento à identificação do utilizador, pode ser usada, por exemplo, para restringir as máquinas a que um dado utilizador tem acesso. Para que este mecanismo seja fiável é necessário um total controlo da rede ou, então, a existência de um processo de autenticação das máquinas de forma a evitar que um intruso utilize uma máquina não autorizada para simular uma máquina autorizada.

Com a actual tendência de abertura a redes alargadas e a crescente necessidade de partilha e acesso remoto à informação, a quantidade de dados armazenada em bases de dados está a aumentar. Inerentemente a este crescimento aumentam os riscos de segurança. A probabilidade de os utilizadores de um sistema usarem mal a informação depende tanto do seu valor como do número de pessoas que a ele têm acesso.

O controlo de acesso é muito importante em qualquer sistema de cuidados de saúde, quer a informação fique alojada em bases de dados centralizadas ou distribuídas. Neste último caso muito mais pela razão de que a sua gestão é mais difícil.

O facto de que nem todas as pessoas têm acesso aos dados é uma consequência lógica do direito à privacidade. Existem dois tipos de mecanismos de controlo de acesso: controlo de acesso discricionário e o obrigatório. Este último é usado em sistemas de registo clínico electrónico porque exige que todos os utilizadores que têm acesso e gerem informação do paciente sigam regras estabelecidas pelo responsável dessa gestão. A forma mais comum de estabelecer regras é através de listas de controlo de acesso, que armazenam as permissões de acordo com os recursos definidos: quem tem acesso ou não a um recurso.

---

[6] Endereço IP – é a identificação de um dispositivo que usa protocolo IP (Internet Protocol) para ligar-se a outros dispositivos (ou à Internet). Para mais informação RFC 791.

No caso dos sistemas de registo clínico electrónico é muito mais importante o nível de controlo de acesso; este regula o acesso dos utilizadores por perfil (ou níveis de acesso) à aplicação ou base de dados. A este nível, os controlos dependem da aplicação ou base de dados em si. É difícil conciliar a complexidade dos sistemas com a segurança e confiança, razão pela qual é essencial conhecer os utilizadores e os componentes do sistema, para melhor compreender que controlos de segurança específicos devem ser aplicados.

Os utilizadores dos sistemas de registo clínico electrónico devem ser responsabilizados pelas suas acções dentro do sistema. É importante ter um registo de quem, onde, quando tem acesso ao sistema e o que fez, para que acções de recuperação possam ser tomadas quando necessário. No entanto, nestes sistemas a maior parte das vezes essas acções de recuperação serão executadas demasiado tarde e não vão reparar consequências trágicas. É por esta razão que a identificação e autenticação são cruciais. Constituem a primeira barreira para prevenir o uso errado e não autorizado da informação.

A gestão do controlo de acessos tornou-se ainda mais preocupante com a abertura das redes internas das instituições de prestação de cuidados de saúde a redes mais abrangentes (por exemplo, a Internet). Novas regras devem ser aplicadas quando os utilizadores destes sistemas não estão dentro do perímetro da sua rede local (intranet) mas podem estar em qualquer parte do mundo tentando aceder à informação. Deverá haver um equilíbrio entre o que os utilizadores podem realmente aceder e as possíveis novas ameaças a que o sistema possa estar exposto.

Como referido anteriormente, os sistemas de registo clínico electrónico agregam diferentes tipos de informação (por exemplo, imagem médica) que por seu lado, exigem diferentes tipos de controlos de acessos. Definir uma política de segurança adequada, é muito importante neste caso, estabelecendo regras que descrevam que tipo de privilégios de acesso os utilizadores devem ou não ter, de acordo com a sua função dentro da organização. É por isto que para cada utilizador identificado existe a necessidade de determinar os seus privilégios em termos de acesso a serviços ou informação. Uma forma de lidar com o mapeamento utilizador/acção é o uso de um identificador único do paciente (vulgarmente designado por número de processo do paciente). Ele vai ajudar a identificar cada paciente de forma inequívoca e assegura que apenas os dados correctos são anexados ao seu registo. Actualmente também existe um problema comum com o controlo de acesso que é a disponibilidade da informação. Deverá ser sempre possível aceder à informação especialmente durante procedimentos de cuidados médicos críticos (por exemplo, uma urgência). Quando existe alguma falha ou erro no processo de autenticação os utilizadores autorizados podem ficar impedidos de aceder à informação a que têm direito. Outro aspecto importante do controlo de acesso tem a ver com a gestão da informação. A inserção, alteração e eliminação da informação terá

de ser atribuída às pessoas certas e as regras de acesso e práticas têm de ser definidas para limitar o acesso à informação pelo pessoal da gestão, que não tem aptidão na prestação de cuidados médicos. A qualidade dos dados do paciente depende disto.

Ataques como negação de serviços (em inglês, designado por DoS[7]) impedem utilizadores autorizados de desempenharem o seu trabalho e poderão ser a causa de atraso no tratamento ou cuidados médicos ineficazes e consequentemente afectar negativamente a vida ou saúde dos pacientes. A disponibilidade é um assunto crucial. Não é apenas importante controlar e permitir o acesso aos utilizadores certos mas também fornecer acesso e sempre que necessário. Por exemplo, quais poderão ser as consequências de não se disponibilizar o acesso à informação do paciente durante uma consulta? Se um paciente tiver uma constipação e for necessário medicação, o médico ao não ter acesso à informação do paciente, não saberá que tipo de alergias ou reacções o paciente poderá sofrer para essa medicação. O próprio paciente poderá não saber ou lembrar-se especificamente quais são e isto poderá ter consequências no tratamento do paciente.

2.4.1. Ameaças à Segurança e Vulnerabilidades

Uma das mais perigosas ameaças que afecta os sistemas de informação dos serviços de saúde advém do descuido dos seus próprios funcionários. Existem diferentes tipos de pessoas, educação e formação dentro da mesma instituição e há sempre alguns com diferentes tipos de interesses relativamente à informação do paciente. Utilizadores internos são aqueles que têm acesso ao sistema dentro do perímetro da intranet da instituição. Estes são utilizadores autorizados e por essa razão os mais perigosos, conhecem o sistema e trabalham todos os dias com ele, e por isso é-lhes muito fácil ter acesso e corromper os dados conforme a sua vontade. Por vezes, também usam mal a informação por acidente ou classificam mal os dados causando danos.

Outro tipo de utilizadores que podem usar mal os dados do paciente são os utilizadores autorizados que normalmente acedem ao sistema de fora do perímetro da intranet, i.e., via Internet. Eles normalmente têm acesso a serviços dedicados, como linhas de acesso, para se conectarem e executar as suas tarefas.

Um terceiro nível de utilizadores é constituído pelos utilizadores não autorizados. Podem estar dentro ou fora do perímetro e tentar aceder à informação que lhes está vedada. Podem usar várias técnicas e explorar várias fragilidades, por exemplo: engenharia social, divulgação de senhas, ataques de negação de serviços, conexões não protegidas, falhas na instalação do servidor e todos os problemas de segurança relacionados com a autenticação dos utilizadores já referidos.

---

[7] DoS – Denial of Service. Ataque que diminui a disponibilidade dos serviços ou equipamentos.

Outro problema está no controlo de permissões e privilégios atribuídos em cascata. Muitos dos sistemas actuais permitem definir e atribuir privilégios e direitos complexos aos utilizadores, que podem ser passados a outros. Isto pode dificultar a rastreabilidade dos autores de certas acções. Ás vezes também é complicado negar o acesso à informação a alguém que deixa o emprego ou muda de funções.

Finalmente, existem alguns problemas de segurança relacionados com as redes sem fios. É muito prático para os médicos poderem utilizar o equipamento móvel (por exemplo: um PDA[8], um computador portátil, etc.) dentro da instituição. Esta situação está a crescer nas instituições de saúde em Portugal e constitui uma tecnologia muito útil no acesso ao registo clínico do paciente, na elaboração de diagnósticos e passagem de prescrições. No entanto, as redes sem fios estão sujeitas a ameaças de segurança mais difíceis de controlar do que as de uma rede com fios. Não é fácil rastrear utilizadores de uma rede sem fios, e, por esta razão, quando alguém com um equipamento adequado se aproxima de uma rede sem fios e se conecta pode "escutar" toda a informação em trânsito nesse momento se a rede não estiver adequadamente protegida.

Estes são apenas alguns dos problemas mais importantes em termos de segurança no que se relaciona com o controlo de acessos. De seguida são descritas algumas recomendações que podem evitar algumas destas vulnerabilidades de segurança.

2.4.2. Soluções e Mecanismos de Segurança

Para controlar convenientemente o acesso como um todo numa rede de cuidados de saúde podem ser definidos níveis de acesso. Há necessidade de definir explicitamente quem tem acesso e a que informação. A Tabela 1 é apenas um exemplo de como as regras e níveis de acesso podem ajudar na descrição e fornecimento de controlo eficiente quando se acede aos dados clínicos do paciente.

Tabela 1 – Lista de privilégios

Utilizadores	Direitos de acesso
Paciente	Toda a sua informação clínica.
Médico	Toda a informação clínica dos seus doentes relacionada com a sua especialidade.
Enfermagem	Toda a informação relacionada com o seu departamento ou serviço.

[8] PDA - Personal Digital Assistente.

Técnicos	Toda a informação relacionada com o seu departamento ou serviço.
Investigador	Idade, sexo, diagnósticos e procedimentos, informação clínica sem identificação.
Administrativo	Informação administrativa, identificação do paciente

Este tipo de listas pode ajudar a evitar alguns dos incidentes que quebra a confidencialidade e integridade dos dados do paciente e são normalmente feitos dentro da politica de segurança da instituição, cumprindo todas as regras que definem como as pessoas devem agir e que responsabilidade têm no que se refere à segurança.

Os direitos de acesso e utilizadores são definidos pelos perfis de utilizador. Os perfis incluem a profissão dos utilizadores, tipos de dados a que podem aceder, funções ou programas que podem usar. O pessoal administrativo não deve aceder aos dados médicos. Alguns dados médicos ou permissões para modificar dados clínicos e terapêuticos devem estar disponíveis apenas a alguns médicos. Os pacientes também têm uma palavra a dizer sobre o acesso aos seus dados, por isso têm que dar o seu consentimento a quem tem o direito de aceder a essa informação.

Para além disto, se existirem sistemas de gestão que disponibilizem um bom nível de validação de dados conjuntamente com a identificação única do paciente, poder-se-á evitar dados mal classificados aquando da sua inserção e actualização. Regras diferentes devem ser aplicadas aos utilizadores com a função de gestão. Acções tais como actualizações tem que ter regras mais restritas do que aquelas que apenas lêem a informação sem a alterar. É por esta razão que as regras têm de ser aplicadas na medida do necessário, concedendo os privilégios estritamente necessários para executar as suas tarefas correctamente e nada mais. A formação, a autenticação forte e também a encriptação podem ajudar a assegurar que estas regras sejam seguidas, especialmente quando são usadas redes sem fios. Uma lista completa e actualizada de equipamentos, bem como de pessoal que usa e acede à rede é um documento útil a manter.

Um dos meios de enfrentar as mencionadas ameaças externas são as *firewalls*[9]. As *firewalls* ajudam no controlo de acesso porque podem ser configuradas para terem um conjunto de regras que podem permitir ou não alguns tipos de pacotes. Este controlo pode ser feito de acordo com o serviço, utilizador e comportamento. Como existem vários tipos de *firewalls* é necessário seleccionar o mais adequado para o nível de controlo exigido.

---

[9] Firewall – Um firewall ou barreira “corta fogo” é um equipamento colocado na zona fronteira de uma rede, cujo objectivo principal é o controlo de acessos não autorizados oriundos de outras redes, por exemplo, a internet. Especificado pelo RFC 2828.

Antigos utilizadores da rede devem ser desactivados, ou seja, os utilizadores têm que ser excluídos de todo e qualquer acesso que habitualmente detinham. No que se refere à segurança física, o controlo de acesso às instalações da instituição tem que ser assegurado adequadamente para que constitua mais uma barreira a ser ultrapassada no acesso não autorizado à informação.

Por último, neste contexto, é de salientar a norma: ENV 13606 – "Electronic Healthcare Record Communication (EHRcom)", que especifica os privilégios necessários para aceder ao registo clínico electrónico.

2.5. Monitorização, Auditoria e Logs

Hoje em dia é possível usar ferramentas específicas e até automáticas para monitorizar e rastrear os utilizadores de um sistema. O processo de auditoria ajuda a verificar se o sistema e, os seus controlos de segurança estão correctamente instalados e a funcionar como exigido ou desejado. Auditar os "rastos" e *logs* de acesso à informação pode constituir um forte motivo dissuasivo ao abuso. Os registos abrangem detalhes sobre o acesso à informação incluindo a identidade do utilizador, data e hora, fonte e destino, informação pesquisada e retirada e talvez o porquê de aceder aquela informação. A sua eficácia depende essencialmente de quão forte é o processo de identificação. A responsabilização é por isso essencial dentro dos processos de prestação de cuidados de saúde, por forma a evitar acessos futuros indevidos ou incorrectos.

Ainda mais, deverá ser desenvolvida e implementada uma política de segurança com regras afirmando e reforçando o uso correcto de identidades para que a detecção de utilizadores partilhados possa ser eficaz, e os utilizadores possam saber como agir correctamente para seu próprio beneficio como também para com a instituição, e penalizados, se for necessário.

2.5.1. Ameaças à Segurança e Vulnerabilidades

Um dos problemas mais relevantes sobre auditoria é o facto de que quando está a ser feita, deve gerar os seus próprios *logs*, que deverão ser verificados pelos gestores de sistema.

A auditoria está directamente relacionada com o controlo de acesso. De facto, auditoria é uma das principais razões pela qual se faz o controlo de acesso. É uma boa forma de rastrear e contabilizar as acções dos utilizadores dentro do sistema. Assim, se o controlo de acesso é contornado, não está garantida a integridade dos *logs*. Estes podem ser alterados ou apagados para camuflar acessos ou acções não autorizados.

Ter demasiados utilizadores a lidar com os *logs* pode também constituir uma ameaça porque é difícil saber e controlar quem lidou com eles, se a sua integridade foi quebrada e quem pode ser responsabilizado por isso.

Também é possível usar os *logs* para executar outro tipo de ataques. Os *logs* contêm uma grande quantidade de informação relacionada com o utilizador (por vezes, até senhas) que são rastreáveis durante o tempo de conexão. Essa informação na posse de um atacante facilitará a sua actividade.

Outras questões a não esquecer são as relacionadas com a segurança física. Se não forem estabelecidas medidas físicas adequadas, o controlo de acesso pode ser quebrado, e os próprios *logs* podem ser mudados ou falsificados. Se são enviados via correio electrónico ou qualquer outro tipo de software de comunicação em que a informação circula em claro, qualquer pessoa pode facilmente "escutar" a rede, quebrar a confidencialidade dos dados e executar facilmente um ataque. Mais ainda, se for realizada uma cópia de segurança dos *logs*, e estes armazenados fora do sistema onde não haja medidas específicas de segurança física, podem ser facilmente acedidos por qualquer tipo de utilizadores. Os utilizadores autorizados representam algumas das mais perigosas ameaças, não são considerados "estranhos" pelo sistema.

2.5.2. Soluções e Mecanismos de Segurança

Para evitar alguns dos problemas de segurança mais comuns com os *logs*, estes devem ser feitos e analisados regularmente para que a maior parte das acções dentro do sistema possam ser monitorizadas e relatadas frequentemente, evitando desta forma que eventos não detectados passem completamente despercebidos. Esta análise deverá ser feita preferencialmente por ferramentas automáticas e sem intervenção humana para se evitar as mais comuns ameaças de segurança. No caso da intervenção humana ser essencial, todos os controlos de segurança aplicados ao controlo de acessos deverão ser executados como primeiro obstáculo para prevenir a violação da confidencialidade e integridade dos dados.

É muito importante no âmbito da política de segurança definir níveis de controlo de acesso. Mais importante ainda é definir os responsáveis por gerir os *logs* e aplicar-lhes regras específicas, devendo as suas acções relativas aos *logs* também ser auditadas e relatadas ao responsável máximo pela segurança.

Alarmes e notificações imediatas devem ser disponibilizadas para detectar acontecimentos pré-definidos que revelam quebra de padrões de comportamento. Por exemplo, modificação dos registos de um paciente por alguém que não deveria estar a trabalhar a uma determinada hora.

Por último, a segurança física não deverá ser descurada pois constitui o primeiro obstáculo para prevenir o abuso e mau uso da informação. Os *logs* devem ser idealmente armazenados em máquinas que não são usadas em outros trabalhos correntes, por exemplo, mantidos junto a ficheiros ou outros dados que não vão ser acedidos ou usados frequentemente. Devem ser mantidos em local com segurança física adequada, salvaguardados da ameaça humana ou desastres naturais.

Por último, a norma WI 134 ENV [23] – "Accountability and Audit Trail Mechanism for Healthcare Information Systems" providência um conjunto de mecanismos de auditoria e contabilização de *logs*.

2.6. Gestão de Bases de Dados

Com as novas tecnologias disponíveis, grandes volumes de dados podem ser facilmente armazenados e acedidos em grandes bases de dados. Actualmente os sistemas de registo clínico electrónico estão dependentes não só de bases de dados concentradas, mas também de bases de dados distribuídas, e às quais os utilizadores de diferentes departamentos ou serviços podem ter um acesso rápido e eficiente. Seja qual for a forma de armazenamento estas bases de dados podem ajudar em investigações mais avançadas e permitir que dados clínicos sejam partilhados com o objectivo de reduzir o manuseamento de papel e ajudar na execução de tarefas administrativas. O tratamento do paciente pode ser melhorado com o uso de uma base de dados abrangente, clinicamente relevante e digitalmente codificada. A existência de ferramentas de interrogação às bases de dados permite disponibilizar rapidamente conhecimentos sobre indivíduos e grupos de pacientes. Este é um dos principais objectivos dos sistemas de registo clínico electrónico e as bases de dados desempenham um papel fulcral na sua execução. Para o uso de bases de dados relacionais, onde toda a informação é disponibilizada local ou remotamente, a relação entre tabelas é uma característica essencial para implementar o sistema. Para além disto, bases de dados orientadas ao objecto também podem ser usadas para modelar informação clínica de tal forma que o significado de cada elemento de informação é determinado usando um dicionário de dados médicos e que vai constituir um objecto dentro da própria base de dados. Os objectos agregam-se em conjuntos e herdar propriedades de outros objectos. Isto define uma nova forma de relacionar os dados clínicos diferente das bases de dados relacional, mas os objectivos e resultados principais são bastante similares.

2.6.1. *Ameaças à Segurança e Vulnerabilidades*

As bases de dados estão expostas a graves ameaças e vulnerabilidades. Os dados podem ser corrompidos não só pelos utilizadores ou por programas (por exemplo, vírus), mas também por causas externas, tais como falhas de energia ou problemas nos equipamentos. Tais bases de dados podem necessitar de controlos de segurança adicional devido ao seu rápido crescimento. Pode tornar-se difícil controlar grandes volumes com os diferentes tipos de informação que os sistemas de registo clínico electrónico podem conter. No que se relaciona com o armazenamento de dados de pacientes, a integridade é muito importante porque uma alteração mínima pode afectar a vida e os cuidados médicos a receber. Problemas de inconsistência podem ocorrer frequentemente em bases de dados devido a falhas nos programas, vírus ou outros problemas técnicos. Os dados podem ser corrompidos, por exemplo, por uma falha de energia. Transacções que não foram devidamente terminadas podem afectar todo o estado de integridade da base de dados. Para além disto, a redundância de dados pode ser perigosa pois pode propiciar o aparecimento de inconsistências e permitir, por exemplo diferentes tipos de tratamento do paciente dependendo da pesquisa na base de dados.

Devido ao uso da Internet e da interoperabilidade de várias redes para aceder aos registos electrónicos do paciente, ataques que provoquem indisponibilidade de serviços tornaram-se comuns actualmente. Neste tipo de ataques, os servidores ficam impedidos de trabalhar, por exemplo, quando são bombardeados com pedidos adicionais, os quais não têm tempo de atender, e tornam-se incapazes de disponibilizar os seus serviços habituais. São muito difíceis de prevenir e as suas consequências podem ser devastadoras, por exemplo, nos departamentos ou serviços de emergência onde a disponibilidade da informação dos pacientes é vital.

As bases de dados destinadas à investigação podem ser uma fonte de ameaças à privacidade. Por vezes, é possível obter identificação dos pacientes quando as pesquisas certas são feitas. Mesmo não existindo informação específica pode ser possível reconstruir a identificação dos pacientes nas bases de dados de onde a identificação foi extraída. Através deste fenómeno, designado por inferência, é possível deduzir informação a partir de dados que separadamente nunca dariam informação sobre a identificação do paciente.

Outra questão pertinente que pode influenciar directamente as vidas das pessoas, é a definição de quem tem acesso às bases de dados de informação dos registos clínicos do paciente. Por exemplo, se as companhias de seguros tiverem acesso a dados de saúde dos seus clientes, podem negar-lhes seguros; do mesmo modo, os empregadores podem despedir ou não contratar pessoas baseados no mesmo tipo de informação.

Por último, outro aspecto da segurança que não pode ser relegado para segundo plano é o da segurança física. As tecnologias e os controlos de segurança mais avançados serão ineficazes se, por exemplo, alguém tiver acesso à sala onde se localiza o servidor que armazena a informação dos pacientes, podendo roubar o equipamento ou mesmo destruí-lo e torná-lo inacessível. O mesmo se aplica às cópias de segurança. Se o atacante lhes tiver acesso, pode reconstruir toda a informação que a instituição que presta cuidados saúde recolheu durante anos.

2.6.2. Soluções e Mecanismos de Segurança

Para prevenir ou minimizar algumas das ameaças e vulnerabilidades identificadas anteriormente há algumas medidas que poderão ser adoptadas.

Em caso de falhas ou até no caso de ataques por negação de serviços, torna-se importante a existência de repositórios de armazenamento de dados em duplicado que constituem uma cópia para ser acedida e usada se a que está em serviço necessitar de ser reposta. Este segundo equipamento, a ser usado no caso de emergência, deve ser sempre mantido em sincronismo com o equipamento principal. Deverá estar localizado numa área reservada com controlos específicos de segurança, no que concerne aos acessos e autenticação.

O uso de sistemas de gestão de bases de dados bem testados pode também contribuir para a segurança dos dados e para que falhas nos programas não aconteçam tão frequentemente ou possam ser melhor controladas. Medidas de gestão e controlo de qualidade de dados podem ajudar eliminar informação redundante ou incorrecta relacionada com os pacientes.

As cópias de segurança e os registos das transacções deverão ser mantidos actualizados e feitos regularmente, assim como armazenados em local seguro, porque podem ser a única forma de recuperar na totalidade e com consistência a base de dados depois de ocorrer uma falha. Actualmente, a maior parte dos sistemas de gestão de bases de dados possui ferramentas específicas para fornecer arquivo e armazenamento de informação automaticamente e regularmente. Também é importante ser capaz de armazenar e contabilizar transacções rejeitadas para que as tentativas de quebrar a privacidade possam ser detectadas facilmente e possam ser feitas correcções para melhorar a sua eficiência.

Para minimizar ataques bem sucedidos poderão ser adoptadas algumas medidas já referidas (por exemplo, instalação de barreiras que separam o tráfego interno e externo da rede tais como

firewalls, sistemas de detecção de intrusão tais como, IDS[10] e auditorias frequentes do tráfego da rede). Embora a eficácia dos programas de antivírus[11] não seja muito elevada, eles podem ser desenvolvidos rapidamente e prevenir a maior parte dos vírus conhecidos.

A duplicação da base de dados, quando exista, nunca deve ser acessível por qualquer máquina do sistema, a não ser a base de dados central. A replicação deve ser feita automaticamente e em horas de pouco tráfego.

Deverá também existir uma outra barreira (por exemplo, outra *firewall*) entre o servidor aplicacional e a base de dados de registos clínicos; desta forma, se o servidor aplicacional é atacado, existe outro obstáculo a ser ultrapassado para atingir o servidor da base de dados.

Como foi mencionado anteriormente, existe um grande problema relacionado com o acesso às bases de dados para investigação, em que a informação pode ser inferida mesmo quando esta foi devidamente processada para que os pacientes não tenham uma identificação directa. Um tipo de protecção poderá passar por especificar um número mínimo de campos a pesquisar e nunca permitir aos utilizadores interrogar todos os registos de uma só vez.

O primeiro passo na protecção de sistemas de informação é a segurança física, pois pode prevenir ataques tais como roubo ou destruição de equipamento. No caso das bases de dados dos pacientes, estas deverão ser colocadas em locais controlados onde apenas pessoal autorizado possa aceder. Meios de autenticação suplementares, tais como dispositivos biométricos, podem ser utilizados nestes casos. Quando nenhum dos obstáculos físicos funciona, a cifragem pode ser uma solução para impedir o acesso a utilizadores não autorizados. A cifragem consiste em codificar a informação a ser armazenada ou transmitida para que apenas os utilizadores autorizados possam compreender os dados (em princípio, nem o gestor da rede não os consiga compreender).

Finalmente, para evitar quebras de segurança, deverá haver uma destruição segura dos dados e de equipamento obsoletos, ou seja, devem ser completamente "limpos" de informação.

Em conclusão, todas estas soluções devem ser consideradas desde o início, mesmo antes da base de dados ser utilizada. Os sistemas de gestão de bases de dados têm alguns controlos de segurança e ferramentas de monitorização que constituem a primeira barreira para algumas das ameaças e vulnerabilidades que enfrentam. Todas as outras soluções dependem também do ambiente

---

[10] IDS – Intrusion Detection System. Sistema de detecção de intrusão, é definido como sendo um serviço que monitora e analisa eventos de uma rede e providencia alertas em tempo real de acessos aos recursos da rede não autorizados. Para mais informação ver o RFC 2828.

[11] Antivírus – Os programas de antivírus fazem análise de ficheiros recém-chegados da Internet tentando neles detectar código malicioso.

e objectivos do sistemas da base de dados, ou seja, por exemplo, se vai ser ou não exposto a um ambiente hostil como a Internet.

2.7. Gestão das Comunicações

O acelerado desenvolvimento da tecnologia de comunicações disponibilizou tanto novas oportunidades como ameaças e vulnerabilidades à prestação de cuidados de saúde. Com o uso alargado da telemedicina é mais fácil e mais rápido comunicar entre instituições de prestação de cuidados médicos e respectivos profissionais de saúde para troca de opiniões e conhecimento. Comunicações de dados eficientes e efectivas são vitais para os sistemas de gestão de saúde devido à necessidade imperativa de partilha de informação pelos profissionais de saúde. As redes de computadores tornaram-se largamente usadas porque permitem estas comunicações da forma rápida e fácil, e podem agregar diferentes tipos de dados e tecnologias. No entanto, elas também podem ser a fonte de uma grande diversidade de ameaças à segurança, e apresentam diversas vulnerabilidades e falhas. Todos estes problemas nunca podem ser totalmente solucionados porque a tecnologia está a evoluir tão rapidamente que as soluções de segurança não acompanham o ritmo.

Um volume cada vez maior de bases de dados de cuidados de saúde têm que ser suportadas por boas infra-estruturas de comunicações, tecnologias e programas para que em qualquer situação possam ter o melhor desempenho possível. Ao mesmo tempo, devem fornecer uma troca e armazenamento seguro da informação, de acordo com as necessidades dos sistemas de informação médica.

Melhoramentos tal como o uso de tecnologias *web*, para fornecer aplicações mais fáceis de usar introduziram no entanto ainda mais insegurança. Piorou ainda mais com o desaparecimento de fronteiras definidas num qualquer sistema de informação com o uso da Internet como fonte de recursos e um meio de troca e partilha de conhecimentos médicos. Os protocolos da Internet podem permitir que a informação seja modificada durante a comunicação através da rede, sem que as partes envolvidas disso se apercebam.

Qualquer sistema de informação de cuidados de saúde é suportado por infra-estruturas de rede como base para as comunicações, partilha e acesso à informação que normalmente se encontra em servidores de bases de dados localizados remotamente.

Os sistemas de comunicação compreendem, em regra, diversas camadas, pelo que a segurança nas comunicações deve abranger todas: a camada física; a de ligação de dados; as camadas de rede e de transporte; e a camada de aplicação. A funcionalidade de segurança existente

nas diversas camadas de uma arquitectura de rede de comunicações deverá garantir no seu conjunto, o nível de segurança pretendido em termos de confidencialidade, integridade, autenticação, controlo de acessos, disponibilidade e não repúdio.

Em ambientes de elevadas exigências de segurança, como é o caso de um sistema de informação clínica, poderá levar a alguma redundância de funcionalidades de segurança entre as diversas camadas, o que se deverá ter em atenção nas diferentes fases de projecto, de gestão e manutenção das redes informáticas.

A rede informática da saúde em Portugal opera com base nos protocolos TCP/IP[12] e assenta numa arquitectura de rede aberta. Esta infra-estrutura de rede é suportada por diferentes tecnologias e apresenta uma estrutura heterogénea (ver Figura 4).

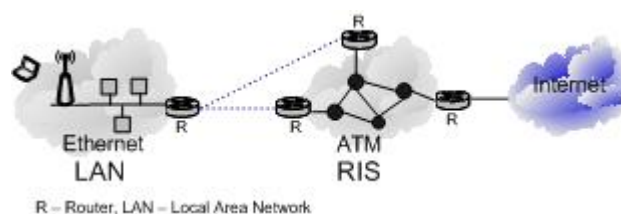



Figura 4 – Representação da rede informática da Saúde

Tipicamente, as redes locais (redes cabladas ou sem fios) das instituições apresentam uma topologia em estrela (ligadas por fibra óptica) e encontram-se conectadas à RIS[13] [78] por circuitos dedicados e linhas RDIS[14]. A distribuição aos utilizadores é feita por cabos em cobre. Por outro lado, a "espinha dorsal" da RIS apresenta-se em tecnologia ATM[15] e conecta-se à Internet em dois pontos de acesso.

De seguida serão enumeradas as formas e/ou tipos de ataques relevantes, serão analisadas as principais vulnerabilidades das tecnologias em causa e serão identificadas técnicas, mecanismos ou protocolos de segurança aplicáveis.

---

[12] TCP/IP – Transmission Control Protocol / Internet Protocol. É uma solução tecnológica usada em redes privadas e de telecomunicações como suporte computacional para um grande número de aplicações, para o desenvolvimento, como plataforma de interconexão e na operação da Internet.

[13] RIS – **R**ede **I**nformática da **S**aúde. É uma rede multimédia de telecomunicações privada do Ministério da Saúde em Portugal.

[14] RDIS – Rede Digital com Integração de Serviços.

[15] ATM – Asynchronous Transfer Mode. Uma rede baseada num conjunto de *switches* ATM inter-conectados por ligações ATM ponto-a-ponto em fibra óptica. Esta tecnologia introduz o conceito de células, endereçamento e circuitos virtuais.

2.7.1. Ameaças à Segurança e Vulnerabilidades

A maior parte das ameaças e vulnerabilidades apresentadas nesta secção são semelhantes às de qualquer outro sistema de informação, porque a rede possui as mesmas características e disponibiliza as mesmas funcionalidades e por isso está exposta aos mesmos problemas de segurança. Segue-se a identificação de algumas das ameaças mais importantes a um sistema de informação clínica.

A escuta do meio físico de transmissão pode ser efectuada por derivação do meio físico, por derivação do próprio meio ou dos nos conectores, por leitura da radiação electromagnética emitida pelos cabos ou por escuta do espectro radioeléctrico. O ataque por bloqueio, normalmente, ocorre por disrupção do meio físico (por exemplo, corte de cabos) ou através do posicionamento de obstáculos entre o emissor e o receptor (por exemplo, no caso das redes sem fios). O desvio da ligação para outro equipamento ocorre com o intuito de aceder a informação ou recursos de comunicação.

As formas de ataque utilizadas numa dada rede ou ligação dependem da natureza do meio físico utilizado. Por exemplo, em meios físicos em cobre (por exemplo, par entrançado) são relativamente fáceis de derivar, desviar, escutar, interromper ou danificar. A execução de derivações em fibra óptica já não é tão fácil, por exigir a interrupção da fibra para inserção de um derivador óptico. Por outro lado, este tipo de meio físico é fácil de bloquear, interromper ou danificar. Não é possível a escuta, pelo facto de que luz utilizada na transmissão, próximo do visível, não ser susceptível de medição do campo electromagnético. No caso de utilização de meios sem fios, ataques por escuta ou bloqueio são bastante fáceis de executar, já que estes meios são bastante sensíveis às condições de propagação e, portanto, estão acessíveis a qualquer dispositivo localizado na área do alcance da rede sem fios.

No caso de a escuta (*sniffing*) ser bem sucedida, a informação pode ser lida directamente ou descodificada, muitas vezes com sucesso, recorrendo a software livremente disponível. Os principais objectivos neste tipo de ataque são, normalmente, a captura de senhas que estejam a circular em claro e o acesso a informação (por exemplo, nomes de pessoas), que permita outro tipo de ataques, por exemplo, do tipo de "engenharia social" (ver descrição mais à frente).

O ataque de escuta representa uma séria ameaça à segurança, pois pode comprometer a confidencialidade dos dados do paciente em trânsito, por exemplo, resultados de exames e prescrições médicas estão permanentemente a circular na rede. No entanto, a grande maioria as redes locais das instituições que integram a rede informática da saúde em Portugal funcionam em

modo comutado, o que reduz fortemente o problema da escuta, dado que entre uma estação terminal e um comutador, só circula tráfego com origem e destino nessa estação, não sendo visível noutros pontos da rede.

Ataques por bloqueio, negação ou indisponibilidade de serviços, são normalmente dirigidos aos servidores e aos equipamentos de comunicação com o objectivo de causar disrupção de serviços. Se atingirem pontos-chave, podem causar consequências graves ao nível da prestação de cuidados de saúde, em particular em serviços de emergência ou cuidados intensivos.

Esta categoria abrange, por exemplo, ataques por disseminação de vírus, *e-mail bombing*, e ataques distribuídos (DDoS). Este tipo de ataques pode ter origem dentro do perímetro de rede ou fora, sendo extremamente difícil de os detectar e localizar.

No caso do *e-mail bombing*, é enviado um grande número de mensagens para a caixa de correio ou listas de distribuição, com o objectivo de congestionar os servidores de correio electrónico, as caixas de correio ou os circuitos de acesso. As soluções para este tipo de problemas passam, por exemplo, pela instalação de filtros de correio electrónico e a utilização de mecanismos *anti-spam*[16].

Os ataques ao equipamento de rede pretendem explorar vulnerabilidades específicas dos componentes (por exemplo, sistemas operativos, encaminhadores, nós de comutação, servidores de nomes, etc.) ou dos protocolos da rede. É frequente que em certos tipos de equipamentos de rede (por exemplo, *router*[17]) sejam deixadas "portas traseiras" originalmente concebidas para desenvolvimento ou testes. Quando descobertas, podem ser utilizadas para obter acesso privilegiado ao equipamento por parte de utilizadores não autorizados. Soluções para este tipo de vulnerabilidades passam pelo acompanhamento de listas de segurança e a instalação de *patches* de correcção do problema.

As redes dependem do funcionamento de DNS[18] através do qual nomes familiares (por exemplo, www.min-saude.pt) são convertidos em endereços da rede abstractos (por exemplo,

---

16 Anti-spam – O termo SPAM é usado para referir-se a correio electrónico não solicitado, que geralmente é enviados para um grande número de pessoas. O uso de filtros *anti-spam* permite atenuar este tipo de ataque (ou, melhor, prática muito incomodativa).

17 Router – O *router* ou encaminhador é um dispositivo para interligação de redes de diferentes tecnologias que fazem o encaminhamento e a comutação dos pacotes entre si.

18 DNS – Domain Name System. O serviço DNS permite que as máquinas na rede sejam identificadas por um nome, para além da identificação pelo endereço IP.

193.164.0.15) e vice-versa. Caso haja uma falha numa parte do DNS, não será possível localizar alguns sítios *web* e os sistemas de encaminhamento de correio electrónico poderão deixar de funcionar. A corrupção dos servidores raiz do DNS ou de outros servidores de nomes de topo pode conduzir a perturbações generalizadas na rede informática da saúde.

Os ataques a equipamentos podem, ainda, ser feitos à custa da exploração de vulnerabilidades em certas implementações de protocolos. Por exemplo, em vários sistemas operativos a recepção de pacotes IP com tamanho superior a 64 Kbytes causa o "estouro" do sistema.

Existe também uma grande variedade de ferramentas que exploram o funcionamento dos protocolos TCP/IP para provocarem perturbações ou mesmo interrupções do serviço. Por exemplo, ataques por geração continuada de *ping* e ataques por pacotes com endereços falsificados podem ser usados para organizar ataques distribuídos. Neste caso o ataque é lançado em simultâneo de várias origens.

Este tipo de ataques num sistema de informação de saúde, nomeadamente em departamentos de cuidados intensivos ou de emergência médica, em que as comunicações e os serviços têm que ser mantidos permanentemente, poderá ter consequências graves. Neste caso a disponibilidade é o aspecto de segurança mais importante.

Os ataques por *Spoofing* ou "fingimento" consistem na falsificação da identidade de uma máquina, que se faz passar por outra, na tentativa de ganhar acesso a recursos, ganhar acesso a informação ou provocar indisponibilidade de serviços. Este ataque pode ser efectuado ao protocolo ARP[19] ou por alteração do endereço MAC[20] das placas de interface com a rede. Por exemplo, ataques de *ARP spoofing*, *IP spoofing*, *DNS spoofing*, *spoofing* de aplicações e *spoofing* de utilizador. Os ataques por modificação são pouco vulgares nas redes locais dado que, devido ao funcionamento em modo comutado, tal exigiria a modificação de tabelas de encaminhamento dos comutadores, o que seria praticamente impossível.

Este tipo de ataque, que pode ser usado para facilitar outro tipo de ataques descritos nesta secção, também pode ter origem dentro ou fora do perímetro da rede da instituição ou fora.

---

[19] ARP – Address Resolution Protocol. O protocolo TCP/IP que relaciona dinamicamente um endereço IP (endereço lógico) com um endereço MAC (endereço físico). O ARP é usado dentro de um segmento de rede e é limitado a redes que suportam *broadcast*.

[20] MAC – Media Access Control. É um protocolo de baixo nível, implementado em hardware, usado para acesso à rede. O termo MAC address é geralmente usado como sinónimo de endereço físico.

Como foi referido anteriormente (ver Figura 4 – Representação da rede informática da Saúde) as infra-estruturas de redes locais das instituições de saúde conectam-se à RIS através de circuitos dedicados ou linhas RDIS. Por natureza, estes canais não implementam segurança, pelo que esta deverá ser implementada nos extremos (i.e., nos *routers*). Como a rede ATM [4] é fundamentalmente orientada à conexão, isto significa que uma conexão virtual tem de ser estabelecida antes de qualquer transferência de dados: logo, há um mito de opção por mecanismos fracos ou inexistentes em termos de autenticação ou encriptação que decorre de dois factores. O primeiro é a ideia de que a utilização de circuitos virtuais constitui um isolamento contra a generalidade de ataques; no entanto, por si só, isto não oferece, protecção contra escuta, desvio ou modificação nos extremos da ligação (por exemplo, na rede do operador). O segundo factor prende-se com a questão da segurança entre camadas de software protocolar, que sugere não haver necessidade de replicação de mecanismos na camada de ligação de dados, dado a existência de soluções de autenticação e encriptação nas camadas superiores.

A segurança no nível da camada protocolar de aplicação tem por objectivos a garantia da confidencialidade e integridade dos dados das aplicações, a autenticação dos utilizadores, o não repúdio da utilização dos serviços, o controlo de acesso aos serviços e a sua disponibilidade.

Os computadores funcionam com software. Infelizmente, o software pode também ser utilizado para desactivar um computador e apagar ou alterar dados. Se um computador tiver funções de gestão de uma rede, o seu mau funcionamento pode ter sérias consequências. Um vírus é uma forma de software malicioso. É um programa que reproduz o seu próprio código, introduzindo-se noutros programas de modo que o código do vírus é executado quando o programa infectado é executado. Os vírus podem ser muito destrutivos, como revelam os altos custos associados a alguns ataques recentes (por exemplo, 'I Love you', 'Melissa' e 'Kournikova'). Este problema pode afectar rapidamente toda a rede. Infecções por vírus podem ser facilmente adquiridas através da rede, nomeadamente via correio electrónico ou transferência de ficheiros.

Existem vários outros tipos de software malicioso: alguns causam danos apenas no computador em que foram copiados e outros difundem-se para outros computadores em rede. Por exemplo, há programas (denominados 'bombas lógicas') que se mantêm em hibernação até serem activados por um evento, como uma data específica (por exemplo, sexta feira 13).

Outros programas, conhecidos como "Cavalos de Tróia", aparentam ser benignos, mas, quando utilizados, lançam um ataque malicioso. Outros programas (denominados "vermes") não infectam os restantes programas como os vírus, mas criam réplicas de si próprios que, por sua vez, continuam a reproduzir-se até afogar o sistema.

Outra questão relacionada com a segurança em redes é a ocorrência de eventos ambientais e não intencionais causados por: desastres naturais (por exemplo, trovoadas, inundações, incêndios, sismos); terceiros sem relação contratual com a instituição (por exemplo, interrupção do serviço por obras de construção); terceiros com relação contratual com a instituição (por exemplo., falhas de hardware ou software em componentes ou programas fornecidos); erro humano ou gestão deficiente do operador (incluindo o fornecedor de serviços) ou do utilizador-administrador (por exemplo, problemas na gestão da rede, instalação incorrecta de software).

Os desastres naturais causam perturbações na disponibilidade das redes e podem acontecer a qualquer momento e sem aviso. Em poucos instantes pode desaparecer informação guardada durante anos podendo afectar a prestação de cuidados de saúde, não apenas no momento em que o desastre ocorre, mas também durante o tempo em que a informação fica indisponível. Infelizmente, é justamente durante estes eventos que é mais necessário o funcionamento das linhas de comunicações.

As falhas do hardware e uma deficiente concepção do software podem criar vulnerabilidades que originam perturbações imediatas ou são exploradas pelos atacantes. Como exemplo, *buffer overflow* é uma das vulnerabilidades de que um atacante pode tirar vantagens. Este ataque consiste em colocar a um servidor pedidos excedendo o seu tamanho do *buffer*. Por falha da aplicação, os pedidos, correspondentes a código, são escritos para além do que deveria ser e abrangem a a zona de instruções do processador, que acaba por executar código dos invasores permitindo-lhes ganhar controlo da máquina. Esta ameaça poderá ter consequências graves, por exemplo, caso ocorram em sistemas críticos de suporte de vida. Uma má gestão da capacidade da rede pode conduzir a congestionamentos que entravam ou perturbam o funcionamento dos canais de comunicação.

Ataque por “engenharia social” é a técnica (ou arte) de se aproveitar a boa fé das pessoas para obter informações que possibilitem ou facilitem o acesso aos recursos computacionais de uma organização por parte de utilizadores não autorizados. Entre as informações mais procuradas destacam-se as seguintes: senhas de acesso; topologia da rede; endereços IP e nomes de computadores em uso; nomes de *hosts* em uso; listas de utilizadores; tipos e versões de sistemas operativos usados; tipos e versões de serviços de rede usados; dados sigilosos sobre produtos e processos da organização.

Existem diversas formas de se efectuar um ataque de engenharia social, mas todas elas têm em comum a característica de usarem basicamente a psicologia e a perspicácia para atingir os propósitos do atacante. Actualmente, as mais populares são: o uso do telefone ou correio electrónico para se fazer passar por uma pessoa (geralmente alguém da equipa de suporte técnico ou um

superior da pessoa atacada) que precisa de determinadas informações para resolver um suposto problema; aproveitar informações divulgadas num fórum público da Internet (por exemplo, grupos de discussão) para resolver um problema de rede; enviar programas maliciosos ou instruções com o objectivo de abrir "brechas" na segurança da rede ou recolher o máximo de informações possível sobre esta.

Como referido anteriormente, a melhor forma de prevenir este tipo de ataques é sensibilizar os utilizadores e administradores de rede e sistemas sobre a forma como devem agir nestas situações. A política de segurança da instituição desempenha um papel importante neste sentido, pois é nela que devem ser definidas as normas e procedimentos de protecção da informação.

2.7.2. Soluções e Mecanismos de Segurança

Num projecto de redes informáticas num ambiente de prestação de cuidados de saúde dever-se-á ter em atenção os tipos de ataques e fragilidades anteriormente identificadas, que condicionarão os meios físicos a utilizar, as topologias de rede, a protecção física dos meios de comunicação e o nível de redundância.

Na fase de funcionamento de uma infra-estrutura de rede num ambiente de prestação de cuidados de saúde, é desejável a utilização de mecanismos de segurança adicionais ao nível físico e na camada física, por exemplo, mecanismos de autenticação dos intervenientes na comunicação baseados na utilização de cartões inteligentes. Com o objectivo de maximizar a segurança, poderão ainda ser adoptados outros procedimentos, como por exemplo, efectuar registos de todas as acções de instalação e configuração da rede, verificar todas as ligações físicas existentes na rede e desactivá-las quando não são necessárias. Dever-se-á ainda manter um inventário de todo o equipamento ligado à rede. As salas técnicas, onde se encontra o equipamento de comunicações e servidores deverão ter acesso controlado. Dever-se-á, ainda, efectuar inspecções periódicas do estado da cablagem e dos circuitos de ligação com o exterior. Além das medidas apontadas anteriormente, dever-se-á ainda efectuar auditorias de segurança, envolvendo, por exemplo, a inspecção visual de todos os componentes da rede, dos circuitos de ligação ao exterior e equipamento de comunicação sem fios. Num ambiente crítico, por exemplo, numa unidade de cuidados intensivos, também é muito importante a medição das fontes de emissão electromagnética e dos níveis de interferência electromagnética com o equipamento médico.

Além disto, poder-se-á adoptar outras medidas de protecção contra o bloqueio. Deverá ser utilizada redundância dos meios físicos para que qualquer quebra de um determinado circuito de comunicação não ponha em causa o funcionamento de toda ou parte da rede. Em relação à utilização de meios em cobre, em termos de meio físico, a opção por fibra óptica traz vantagens. Em termos de

topologia, deverão ser adoptadas soluções em estrela. Por outro lado deve ser dada atenção adequada à protecção dos meios de comunicação, por exemplo, utilização de tubagens e calhas embutidas ou enterradas, restringindo o acesso a zonas técnicas e zonas de bastidores de rede.

Ao nível da camada de ligação de dados e transporte, e no caso das redes locais, para prevenir os ataques identificados podem ser utilizadas várias soluções mas, como é natural, nem todos os problemas de segurança ficam resolvidos a este nível e terão que ser tratados nas camadas superiores.

Algumas das soluções poderão passar pela preferência por tecnologia comutada e utilização de VLANs[21] que permitem a criação e isolamento de grupos de máquinas separando o tráfego do resto da rede; utilização de sistemas IDS e auditoria do funcionamento da rede, com o objectivo de monitorizar e detectar padrões anormais de tráfego e a actividade de eventuais *sniffers*; criação de zonas de rede desmilitarizadas (DMZ[22]) para ajudar a prevenir algumas das ameaças referidas.

A par de uma grande variedade de aplicações existe uma grande diversidade de soluções para garantia de segurança no nível de aplicação, por exemplo: autenticação com base em certificados digitais X.509[23]; autenticação de serviços com *Kerberos*[24]; transacções electrónicas seguras através do protocolo SET[25]; correio electrónico seguro através dos padrões S/MIME[26] ou PGP[27]; uso de SSH[28] para o estabelecimento de um canal seguro para transferência de ficheiros ou de outros protocolos; acesso a servidores seguros através do protocolo S/HTTP[29], que permite o estabelecimento de sessões seguras de troca de informação. Além disto existem ainda ferramentas

---

[21] VLANs – Virtual Local Area Network. Uma rede local virtual, é uma rede logicamente independente. Várias VLANs podem coexistir num mesmo comutador (switch). Um outro propósito de uma rede virtual é restringir acesso a recursos de rede.

[22] DMZ - DeMilitarized Zone ou "Zona Neutra" corresponde ao segmento, parcialmente protegido, que se localiza entre redes protegidas e redes desprotegidas e que contém todos os serviços e informações para clientes ou públicos.

[23] Certificados Digitais – Um certificado digital pode ser definido como um documento electrónico, assinado digitalmente por uma terceira parte confiável, que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

[24] Kerberos – É um protocolo de autenticação especificado no RFC 1510.

[25] SET – Secure Electronic Transactions. É um conjunto de protocolos e mecanismos de segurança que permite a realização de transacções seguras com cartão de crédito através da internet.

[26] S/MIME – Secure Multipropose Internet Mail Extensions. Para mais informação RFCs 2311 e 2312.

[27] PGP – Pretty Good Privacy. É um programa criptográfico usado no correio electrónico, especificado pelo RFC 2015.

[28] SSH – Secure SHell. Especificada pelo RFC 793

[29] S/HTTP – Secure Hyper Text Transfer Protocol, especificado pelo RFC 2660.

complementares de segurança, por exemplo, ferramentas de auditoria, *firewalls* e *proxies*[30] de aplicação.

O objecto da autenticação com base dos certificados digitais X.509 é o da autenticação de entidades (por exemplo, pessoas, empresas, máquinas, serviços ou outras). Os certificados são emitidos por autoridades de certificação e são assinados com a chave privada da entidade emissora. A verificação da autenticidade do certificado é feita com a chave pública da autoridade certificadora que emitiu o certificado. Autenticação através de certificados digitais é usado em várias aplicações e protocolos como, por exemplo, o SET, o S/MIME, o SSL[31] e o IPsec[32].

A arquitectura IPsec funciona ao nível da rede e pode ser usada, por exemplo, para o estabelecimento de sub-redes seguras dentro de uma rede ou para suporte de acesso seguro de utilizadores remotos através da Internet. No caso de uma rede de prestação de cuidados de saúde, o mais usual seria o controlo de acesso a utilizadores remotos. Quando esta arquitectura é implementada nas *firewalls* ou nos *routers* de fronteira de redes privadas permite a constituição de canais de elevado nível de segurança, nos quais o tráfego circula autenticado e cifrado.

Como foi referido anteriormente, as redes sem fio apresentam vulnerabilidades de segurança diferentes das redes de cablagem. Algumas melhorias de segurança poderão passar pela utilização do protocolo IEEE 802.11, que se baseia na autenticação de utilizadores e na confidencialidade da comunicação através da utilização do mecanismo de segurança conhecido por WEP[33], nativo para redes móveis. O WEP utiliza um mecanismo de chaves partilhadas com cifra simétrica designado RC4 [5]. No entanto o WEP apresenta deficiências técnicas, sendo possível quebrá-lo em pouco tempo. Mas, apesar das suas vulnerabilidades ter WEP é melhor do que não ter qualquer protecção. De preferência, a chave deve ser alterada regularmente, em especial quando se pretende revogar as permissões de acesso de um utilizador. Só se deve utilizar o WEP se não for possível actualizar os equipamentos para WPA[34] ou WPA2[35]. Esconder o SSID[36]: com esta medida evita-se que o ponto de

---

[30] Proxies – Firewalls de aplicação ou simplesmente proxies, todo o tráfego interno ou externo à rede é encaminhado para o proxie, que funcionando ao nível de aplicação, pode executar funções de autenticação, controlo de acesso, etc.

[31] SSL – Secure Socket Layer. O protocolo SSL mantém a segurança e integridade do canal de transmissão através da Internet, em conexões do tipo TCP, usando cifragem, autenticação e mensagens com código de autenticação.

[32] IPsec – Internet Protocol Secure. O protocolo IPsec oferece para ambientes TCP/IP mecanismos de segurança (autenticação e encriptação) ao nível IP. Para mais informação RFC 2401.

[33] WEP - Wired Equivalent Privacy. O padrão IEEE 802.11 utiliza o protocolo WEP na camada de enlace para autenticar e criptografar os dados que serão transmitidos na rede sem fio.

[34] WPA – Wireless Protected Access. Também chamado WEP2, ou TKIP (Temporal Key Integrity Protocol), Wi-Fi Protected Access. O WPA foi desenhado para ser compatível com o próximo padrão IEEE 802.11i.

acesso anuncie a rede. O intruso terá, portanto, mais dificuldade em conhecer o identificador da rede a que se associar. Por filtragem dos endereços MAC, conhecendo-se de antemão os endereços do equipamento que acedem à rede, é possível configurar o ponto de acesso para permitir acesso apenas a certos endereços. Um intruso poderá porém mudar o seu endereço MAC para coincidir com um endereço MAC que saiba ser permitido na rede.

Desligar os pontos de acesso quando não estiverem em uso: com esta medida reduz-se o tempo de exposição da rede a ataques, sendo também mais provável detectar utilizações anómalas da rede como por exemplo tráfego extraordinário no ponto de acesso, que se pode detectar pelo piscar mais frequente da luz avisadora de actividade de rede.

Outras medidas poderão ser adoptadas para segurança forte, WPA ou WPA2. O WPA foi criado para substituir o WEP que, como foi referido, tem vulnerabilidades de segurança graves. Sempre que possível deve usar-se WPA2 ou WPA como mecanismo de segurança, exigindo que novos equipamentos tenham capacidade WPA2, ou actualizando os equipamentos existentes para essa tecnologia. O WPA2 quando configurado e utilizado correctamente, designadamente do que diz respeito à escolha de chaves ou senhas, não apresenta vulnerabilidades de segurança conhecidas actualmente. O WPA e WPA2 são semelhantes havendo porém excepções, designadamente no algoritmo de cifra, onde o WPA2 apresenta um algoritmo mais forte do que o WPA, o AES[37].

Uma solução para contornar as fragilidades de segurança de redes sem fios é a configuração de VPNs[38], por exemplo baseadas em IPsec, as quais funcionam por cima do nível de rede estabelecendo a sua própria arquitectura de segurança. Com VPN, a rede sem fios pode funcionar em modo aberto ou com uma chave WEP. Tal rede não tem saídas que possam ser exploradas por eventuais intrusos. A saída da rede é pelo concentrador VPN, que é um equipamento considerado seguro que apenas dá serviço a utilizadores autenticados.

No caso dos circuitos dedicados RDIS de interligação das redes locais das instituições com a RIS poderão ser implementadas algumas medidas tais como: o uso de VPNs, IPsec, cifragem da

---

[35] WPA2 – Wi-Fi Protected Access. Compatível com o padrão 802.11i, com mecanismos ainda mais fortes de autenticação e criptografia do tráfego. Utiliza o algoritmo de criptografia AES.

[36] SSID – Service Set Identifier. Nome usado pelo ponto de acesso para se anunciar na rede sem fios.

[37] AES – Advanced Encryption Standard. Baseado num algoritmo de chaves privadas, não existem ataques efectivos conhecidos contra o AES.

[38] VPN – Virtual Private Network. Definida pelo RFC 2828 como sendo uma conexão de computadores de uso restrito, que se estabelece sobre uma estrutura física de uma rede pública, como por exemplo a internet.

informação, acesso e implementação de sites seguros, o uso de MPLS[39] nos *routers* (é uma tecnologia emergente que, além de possibilitar um aumento no desempenho do encaminhamento de pacotes, facilita a implementação da qualidade de serviço, a engenharia de tráfego e VPNs), etc. Por exemplo, nos casos em que é necessário fazer telemedicina para fora da RIS poderão ser usadas VPNs através de linhas RDIS.

Os ataques aos servidores DNS são, em princípio, facilmente controlados com extensões aos protocolos DNS seguro baseado em criptografia de chave pública. No entanto, tal implica a instalação de novo software nas máquinas clientes, pelo que esta solução não se tem generalizado. Além disso, é necessário tornar mais eficaz o processo administrativo que permite aumentar a confiança entre domínios DNS.

Os ataques ao sistema de encaminhamento (*routers*) são bem mais difíceis de contrariar. A Internet foi concebida para maximizar a flexibilidade no encaminhamento, dado que tal reduz a probabilidade de o serviço se perder caso uma parte da infra-estrutura da rede fique inoperante. Não existem meios eficazes para tornar seguros os protocolos de encaminhamento, especialmente nos encaminhadores da espinha dorsal.

O volume de dados transmitidos não permite uma filtragem pormenorizada, pois uma verificação deste tipo praticamente obrigaria à paragem das redes. Por este motivo, as redes só executam funções básicas de filtragem e controlo do acesso, sendo as funções de segurança mais específicas (por exemplo, a autenticação, a integridade e cifragem) executadas nas fronteiras das redes, ou seja, nos terminais e nos servidores de rede que funcionam como pontos terminais.

Para fazer face à execução de software malicioso, a principal defesa consiste na utilização de software antivírus, disponível sob várias formas. Por exemplo, os detectores e desinfectantes de vírus identificam e eliminam os vírus conhecidos. O seu ponto fraco principal reside no facto de dificilmente fazerem frente aos novos vírus, mesmo quando actualizados periodicamente. Outro exemplo de defesa antivírus é o verificador de integridade. Para infectar um computador, um vírus deve introduzir alterações no sistema. A verificação de integridade poderá identificar essas alterações, mesmo quando são causadas por vírus desconhecidos.

Apesar da existência de produtos de defesa relativamente bem desenvolvidos, os problemas com o software malicioso têm aumentado. Existem para tal duas razões principais. Em primeiro lugar, a abertura da Internet permite que os atacantes aprendam uns com os outros e desenvolvam métodos para contornar os mecanismos de protecção. Em segundo lugar, a Internet continua a crescer e a ganhar novos utilizadores, muitos dos quais não têm consciência da necessidade de tomar

---

[39] MPLS - Multiprotocol Label Switching, o principal objectivo é a integração dos paradigmas de troca rótulos com o nível tradicional de roteamento em redes. Os fundamentos do MPLS estão especificados no RFC 3031.

medidas preventivas. Nas instituições de saúde existe uma grande diversidade de utilizadores com acesso à Internet, uns mais bem intencionados outros menos e, por isso, a segurança depende do grau de utilização ou eficácia do software de protecção.

No sentido de minimizar o risco dos incidentes ambientais em redes locais deverão existir procedimentos e regras específicas de forma a salvaguardar informação sensível e vital da saúde do paciente. Por exemplo, no caso de incêndio, para além de dever existir protecções físicas, são necessários procedimentos e alarmes para detecção de incêndio. A recuperação deste ou outro tipo de desastres poder-se-á fazer a partir de um sistema redundante (ou cópias de segurança) localizado num espaço físico diferente.

Estes riscos ambientais (por exemplo: trovoadas e temporais) também são bem conhecidos pelos operadores de redes de telecomunicações, que criaram redundâncias e protecções para a infra-estrutura nas suas redes. Para além disto, a existência de um maior número de operadores no mercado devido à liberalização permite que os utilizadores passem para outro operador em caso de indisponibilidade. Estes riscos são uma das principais ameaças à disponibilidade da rede informática de saúde.

A ameaça de falha de alimentação é assunto crucial no que concerne à disponibilidade dos dados dos pacientes. Esta vulnerabilidade poderá ser protegida através do uso de fontes de energia redundantes, por exemplo UPS geradores de energia ou outras formas alternativas de alimentação.

A concorrência entre fornecedores de *hardware* e *software* deve exercer pressão no sentido de melhorar a segurança dos seus produtos. No entanto, a concorrência não é suficientemente forte para suscitar investimentos na segurança, que nem sempre é o elemento essencial nas decisões de compra. As falhas de segurança são muitas vezes descobertas demasiado tarde, quando os danos foram já causados. A preservação de comportamentos de concorrência leal nos mercados das tecnologias da informação criará melhores condições de segurança.

O risco de erros humanos e de erros operacionais pode ser reduzido com melhor formação e sensibilização. A implementação de uma política de segurança adequada ao nível das instituições contribuirá para diminuir estes riscos.

Finalmente, ao nível da normalização, importa aqui realçar o propósito da norma (ver Anexo A) ENV 13608 – "Security for Healthcare Communication", orientada para a segurança no canal de comunicações.

2.8. Conformidade com Ética, Legislação e Normas

Nesta secção abordar-se-á três temas que pela sua natureza estão relacionados. Os temas são a ética, legislação e normas de segurança. A ética porque preenche lacunas deixadas pela legislação, e por esta não ser suficientemente abrangente para cobrir as mais diversas situações. A ética é também um factor de distinção entre organizações pela adopção de diferentes códigos de ética. A adopção de códigos de ética por parte das organizações traduz-se na introdução de alguma normalização na área médica e numa maior transparência e confiança por parte dos utentes.

A legislação é necessária no sentido de regular a actividade no sector da informática médica, e a adopção de normas de segurança é peça fundamental, não só porque faz com que as organizações e os seus serviços prestados se revista de uma maior credibilidade para o paciente mas também porque ela é necessária para fazer cumprir alguns aspectos da lei.

Em Portugal, a Comissão Nacional de Protecção de Dados Pessoais (CNPD[40]) [17], tem por competências controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais e apoia a elaboração de códigos de conduta, como refere a Lei 67/98 de 26 de Outubro para a Protecção de Dados Pessoais no artigo 32º [18]. O principal objectivo da CNPD é controlar e inspeccionar o processamento de dados pessoais no que se refere aos direitos, garantias e liberdades constituídos na lei portuguesa. Toda a regulamentação, legislação da responsabilidade desta comissão e relacionada com a protecção de dados pessoais poderá ser encontrada no seu sítio *web* [138].

2.8.1. Códigos de Conduta

Nas organizações é comum serem adoptados códigos deontológicos (ou códigos de conduta) ou éticos que permitem inserir regras morais pelas quais o profissional deve reger a sua actividade. Um exemplo é a deontologia médica [11].

Neste âmbito, no sentido de garantir a confiança e privacidade dos pacientes e dar qualidade ao seu atendimento surgem entidades cuja actividade é providenciar normas de conduta ou ética. Existem sistemas auto-regulatórios que contêm suporte legal como é o exemplo da "Prescription Medicines Practice Authority" [12] do Reino Unido que, em conjunto com a entidade governamental "Medicines Control Agencie" [13], trabalha no sentido de regular todos os aspectos da prescrição de medicamentos. Distingue-se, ainda, duas entidades, uma na Europa e outra nos

[40] CNPD – Comissão Nacional de Protecção de Dados Pessoais.

EUA, respectivamente a “Health on the Net Fundation” (HON) e a “Internet Health Coalitions” (IHCC).

A HON considera-se a primeira instituição a introduzir um código de conduta para sítios *web* médicos e de saúde, o HONcode. O HONcode define um conjunto de regras [14] que devem ser respeitadas na construção desses sítios, incluído regras relativas à confidencialidade dos dados do utente e validação/justificação dos conselhos médicos e da informação fornecida.

Em 2000 a IHCC criou o “eHealth Code of Ethics” para promover um conjunto de princípios dirigidos à comunidade médica *online* e que protege os direitos de quem consulta a Internet para obter informações relacionadas com a saúde [15].

A informática pressupõe o tratamento automático de informação de saúde, o que, em muitas situações, possibilita o acesso à informação por profissionais ligados à informática. Embora a segurança dos sistemas imponha acessos restritivos à informação clínica, estes profissionais acabam por ter um grande contacto com a informação de saúde. É por isso fácil perceber que estes profissionais de informática são alvos importantíssimos nas questões ético-legais. Com base nestas preocupações a “International Medical Informatics Association” (IMIA), desenvolveu um código de ética para profissionais na área da informática médica [16].

2.8.2. Legislação

A legislação dá enquadramento jurídico a múltiplas situações e rege a actividade dos profissionais (por exemplo, a obrigação do sigilo profissional), mas não é suficientemente abrangente para cobrir todas as situações, o que é complementado pelos códigos deontológicos ou éticos.

No domínio da saúde a legislação é muito rigorosa e todos os profissionais desta área estão sujeitos a regras restritivas (no caso dos médicos, definidas pela Ordem dos Médicos). Os profissionais de informática na área de saúde estão sujeitos a leis mais abrangentes como o segredo profissional, a protecção de dados, a privacidade, e outras.

Como exemplo, podemos observar no Código Penal Português [144] alguns artigos de extrema importância neste contexto:

Artigo 195º - Violação do Segredo - “Quem, sem consentimento, revelar segredo alheio (…), profissão (…) é punido (…).;

Artigo 196º – Aproveitamento Indevido do Segredo - “Quem, sem consentimento se aproveitar de segredo (…), profissional (…), e provocar deste modo prejuízo a outra pessoa, é punido (…).;

Artigo 197º - Agravação "As penas previstas nos artigos 190º a 195º são elevadas (…) limites máximos (…) se (…) para obter recompensa ou enriquecimento, (…).

Por seu turno a lei nº67/98 de 26 de Outubro [18] – Lei da Protecção de Dados Pessoais transpõe para a ordem jurídica portuguesa a directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, e trata questões relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

No seu princípio geral, artigo 2º, lê-se, "O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais". Esta lei regula o tratamento de dados pessoais que envolve os direitos dos seus titulares, a segurança e confidencialidade do seu tratamento e movimentação.

Da legislação que se aplica aos registos clínicos electrónicos é de realçar o artigo 35º da constituição que refere: «Todos os cidadãos têm o direito de acesso aos dados informatizados que lhe digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam nos termos da lei». A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis; É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei; A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiriços e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional; Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.

A lei 12/2005 de 26 de Janeiro - Informação genética pessoal de saúde no artigo 3º define a propriedade da informação de saúde detalhando que os dados clínicos são propriedade do utente, sendo as instituições depositários da informação a qual não pode ser utilizada para outros fins que não os da prestação de cuidados e a investigação em saúde e outros estabelecidos pela lei. O titular da informação de saúde tem o direito de, querendo, tomar conhecimento de todo o processo clínico que lhe diga respeito.

No artigo 4º regula o tratamento da informação de saúde: «os responsáveis pelo tratamento da informação de saúde devem tomar as providências adequadas à protecção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à

informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais; As unidades do sistema de saúde devem impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respectivas cópias de segurança, assegurando os níveis de segurança apropriados e cumprindo as exigências estabelecidas pela legislação que regula a protecção de dados pessoais, nomeadamente para evitar a sua destruição, acidental ou ilícita, a alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação; A informação de saúde só pode ser utilizada pelo sistema de saúde nas condições expressas em autorização escrita do seu titular ou de quem o represente. O acesso a informação de saúde pode ser facultado para fins de investigação, desde que o anonimato seja preservado. A gestão dos sistemas que organizam a informação de saúde deve garantir a separação entre a informação de saúde e genética e a restante informação pessoal, designadamente através da definição de diversos níveis de acesso; A gestão dos sistemas de informação deve garantir o processamento regular e frequente de cópias de segurança da informação de saúde, salvaguardadas as garantias de confidencialidade estabelecidas por lei».

2.8.3. Normas

A tendência actual vai no sentido de criar e implementar normas internacionais que permitam e favoreçam a segurança e a interoperabilidade dos sistemas à escala global (ver Anexo A). Os sistemas de informação para a saúde são habitualmente implementados em infra-estruturas heterogéneas e dispersas, o que torna ainda mais importante a existência de normas que facilitem a troca segura de informação.

Do conjunto de normas apresentado é de salientar a norma DICOM, que estabelece uma linguagem comum entre equipamentos de imagem médica (geralmente de marcas diferentes e não compatíveis) e computadores; é comum a nível internacional, e já é usada em Portugal por entidades que implementam o PACS[41]. A norma HL7 desenvolve padrões utilizados como especificações de mensagens de forma a facilitar a comunicação electrónica de dados clínicos entre sistemas heterogéneos na área da saúde. Além destas, é de salientar o trabalho desenvolvido pelo grupo de trabalho CEN/TC 251 WGIII, com realce para as seguintes normas: ENV 12924 – "Security Categorization and Protection of Healthcare Information Systems"; ENV 13608 – "Security for

[41]PACS - Picture Archiving Communication System, sistemas de distribuição, arquivo e comunicação de imagens médicas, que permitem a captação, o armazenamento e a distribuição das imagens e dos relatórios por via electrónica, de forma a estarem disponíveis em qualquer posto de trabalho informático existente na instituição. O PACS está a afirmar-se em áreas como: Radiologia, Cardiologia, Gastrenterologia, Ecógrafia, Dermatologia, etc.

Healthcare Communication"; ENV 13606 [1-3] - "Electronic Healthcare Record Comunications"; EN 12251 – "Secure User Identification for Healthcare – Management and security of authentication by passwords"; ENV 13729 - "Secure User Identification for Healthcare. Strong Authentication using Microprocessor Cards"; EN 14484 – "International transfer of personal health data covered by the EU[42] data protection directive - High Level Security Policy (HLSP)"; EN 14485 – "Guidance for handling personal health data in international application in the context of the EU data protection directive". Do trabalho realizado pelo comité técnico da ISO/TC 215 – WG4 é de realçar: ISO/TS 17090, "Public Key Infrastructure", que descreve a utilização de uma PKI no domínio da informática Médica; ISO 22857 – "Guidelines on data protection to facilitate trans-border flows of personal health information"; ISO/WD 27799 – "Security management in health using ISO/IEC 17799", descreve sobre a gestão da segurança da informação na área da saúde; ISO/TC 18308: 2004 – Requirements for an Electronic Health Record Architecture, que especifica requisitos técnicos e clínicos para uma arquitectura de registos electrónicos de saúde, que suporte o uso, a partilha e intercâmbio dos registos clínicos entre diferentes sectores e países.

Há ainda a salientar o padrão HIPAA[43] [35], que preconiza um conjunto de políticas e procedimentos que garantam a privacidade da informação em formato electrónico e dos sistemas de saúde. Através de um conjunto de regras, o HIPAA pretende controlar o acesso aos sistemas e proteger as comunicações que contenham dados privados de saúde em redes de comunicações. Destas medidas destaca-se: a protecção contra intrusão dos sistemas que contêm informação privada relativas à saúde e, se a informação circular em redes abertas, uso de protecção criptografica; a responsabilização da organização pela integridade dos dados; o uso de certificados digitais, assinaturas digitais, e a autenticação de mensagens; para assegurar integridade dos dados, existência de um documento escrito sobre as tecnologias de informação e suas configurações de componentes de rede, programas de Análise e gestão de risco; etc. Este tipo de certificação HIPAA é bastante eficaz, não só pelo facto de ser uma certificação, pelo que sujeita a controlo e auditorias periódicas, mas também porque é sustentada por legislação e por isso deveria ser adoptada em Portugal.

Sublinha-se ainda o trabalho desenvolvido pela comunidade que integra a fundação openEHR [94] no domínio do processo clínico electrónico, no desenvolvimento de especificações do código fonte aberto, no suporte à formação informática na saúde e na cooperação com o CEN, ISO e HL7.

---

[42] EU – União Europeia.

[43] HIPAA - Health Insurance Portability and Accountability Act (ver Anexo A).

Portugal integra um projecto a nível europeu o EUROEC [96] para a promoção do registo clínico electrónico, designado por PROREC (Promotion Strategy for European Electronic Healthcare Records) que tem como principal objectivo promover e coordenar uma convergência europeia para implementação de processos clínicos informatizados abrangentes, comunicáveis e seguros, através da implementação duma rede Europeia de Centros PROREC [95] [96] partilhando objectivos similares, tendo sido definidos como prioritárias as seguintes áreas de intervenção: arquitectura do PCE; normas e sua aplicação; terminologia e codificação; comunicação e fluxo de informação; segurança, privacidade e protecção de dados; tecnologias de desenvolvimento de *software*; questões organizacionais, culturais e sociais; o processo clínico na investigação; educação, formação, manuais, seminários e conferências; fóruns e relações com organizações europeias e internacionais.

Do ponto de vista da segurança, os diferentes grupos de trabalho preocupam-se com estes aspectos e, em geral, preconizam o uso de certificados digitais, com reforço através de cartões inteligentes e códigos de acesso.

2.9. Grelha de Avaliação de Aspectos de Segurança

Algumas questões revestem-se de uma importância extrema na avaliação da segurança de um sistema de registo clínico informatizado. Por exemplo:

O sistema é seguro? Se me esquecer da senha, será que consigo entrar no sistema? (Se conseguir, não será seguro!).

O sistema respeita os padrões técnicos actuais e a lei do país em relação à Lei de Protecção dos Dados Pessoais?

Prevê-se que contribua para a melhoria da prática clínica?

É interoperável com outras aplicações informáticas de registo clínico? Qual o custo dos mecanismos de segurança? Em termos de *hardware*, *software* e do esforço extra que envolve a sua utilização.

Disponibiliza documentação que permita compreender o que faz e como funciona?

Prevê procedimentos em caso de falha técnica? Poderá essa falha prejudicar algum doente? E se isso acontecer, quem assume a responsabilidade?

Entra em conflito com princípios éticos, por exemplo, o da autonomia do doente para fazer uma escolha informada ou o do direito do doente de esperar que não haja uma divulgação de dados confidenciais?

Sintetizando as questões identificadas ao longo deste capítulo, bem como outras questões genéricas abordadas até ao momento, e com o intuito de avaliar os aspectos de segurança de um sistema de registo clínico, foi definida uma grelha que se encontra no Anexo C em duas partes. Os parâmetros de avaliação foram definidos em torno de quatro aspectos nucleares de segurança: autenticação, confidencialidade, integridade e disponibilidade. Através da grelha parcial C1 – Classes de Aspectos a Avaliar, pode-se observar a forma como cada um dos parâmetros em análise interage com os aspectos de segurança. Outra classe de aspectos importantes em termos práticos é a auditabilidade do sistema, tipo de utilização e conformidade com normas. Um conjunto de aspectos agregados mas não menos importante são as defesas e mecanismos de cifragem e intrusão, as comunicações e a documentação.

2.10. Conclusão

Tal como foi referido anteriormente, é muito difícil integrar os sistemas existentes com os novos, pois dessa integração podem resultar vulnerabilidades de segurança. É de boa prática desenvolver os sistemas de registo clínico já com preocupações de segurança integrada de forma a evitar que surjam problemas à medida que o sistema vai crescendo.

Existem normas e sistemas de codificação que poderão ser usados no processo de desenvolvimento de sistemas de informação para a saúde. Eles podem ser muito úteis de forma a manter a simplicidade e eficiência do sistema, pois podem prevenir redundâncias e inconsistências nos dados do paciente.

Conhecer o sistema e os seus objectivos antes do seu desenvolvimento ou implementação são os primeiros passos para a segurança do sistema.

Os processos de identificação e autenticação são a base para muitos controlos de segurança e procedimentos de trabalho. Por isso, é importante definir, testar e escolher os mecanismos de segurança mais adequados. Existe sempre a necessidade de conhecer o melhor possível o sistema que está a ser desenvolvido ou usado, o que vai ajudar a atingir os objectivos inicialmente definidos. Independentemente do processo estar a ser bem feito, ele poderá não estar a ser feito tão bem quanto deveria. Os utilizadores, a tecnologia, o equipamento e uma boa dose de bom senso são as fases mais importantes deste ambiente. Todas elas são necessárias para se interagir compreender e confiar mutuamente no sistema.

Uma das lições mais importantes a retirar é o facto de que, independentemente da tecnologia avançada usada, os controlos de segurança aplicados nunca são suficientes se não existir segurança física para os completar. A segurança deverá ser pensada como um todo. Deve existir sempre

ligação entre a segurança física e lógica para proteger os servidores e evitar ataques maiores à segurança. Estes ataques podem ter um impacto muito negativo e comprometerem seriamente a qualidade dos serviços prestados ao paciente, para além de também poderem comprometer vários anos de investigação importante.

Na gestão de acessos e disponibilidade, o controlo de acessos é a parte da segurança na qual os utilizadores interagem com o sistema. Por essa razão é o ponto mais fraco no processo da cadeia de segurança. Os utilizadores podem fazer qualquer coisa para evitar a segurança apertada e executar o seu trabalho mais facilmente. O controlo de acesso é uma parte essencial do processo de segurança e terá de haver meios eficazes e eficientes de seleccionar e reconhecer os utilizadores de um sistema. Em sistemas de informação de cuidados de saúde tais como os sistemas de registo clínico, há diferentes tipos de utilizadores dentro do mesmo departamento ou serviço que executam tarefas diferenciadas. Terá de haver uma forma adequada para definir quem tem acesso a quê e isto tem que estar claro dentro da política da instituição.

Os *logs* são um importante instrumento de contabilização das acções de um utilizador autenticado. As ferramentas de controlo de acesso são cruciais num sistema de registo clínico, devendo ser melhoradas e testadas para que possam fornecer uma boa qualidade de logs sem comprometer os dados sensíveis dos pacientes em termos de confidencialidade, integridade e disponibilidade.

Uma rede de comunicações eficiente e eficaz é vital para a partilha e o acesso à informação clínica que frequentemente se encontra em servidores de bases de dados localizados remotamente. O grande volume de dados de cuidados de saúde tem que ser suportado por boas infra-estruturas de comunicações, tecnologias e programas, para que em qualquer situação possam ter o melhor desempenho possível. Ao mesmo tempo devem fornecer uma troca e armazenamento seguro da informação, de acordo com as necessidades dos sistemas de informação clínica.

Importa sublinhar que, hoje em dia, os processos de prestação de cuidados de saúde são caracterizados pela troca de mensagens através de redes heterogéneas e abertas, entre diferentes organizações e fornecedores (hospitais públicos e privados, companhias de seguros de saúde, farmácias, etc.). Toda esta facilidade de apresentação e formatação de dados necessita de estar suportada em sistemas clínicos, sistemas de informação hospitalares e outros sistemas de suporte. Através da utilização de tecnologias de ligação correntes e de normas internacionais do sector da saúde (HL7, DICOM, HIPAA, etc.), a sincronização da informação entre fontes de informação diferentes passa a ser possível, mesmo entre aplicações de origens e fabricantes diferentes.

A política de segurança definida pela organização deverá incluir a segurança das comunicações, adoptando medidas apropriadas para assegurar a confidencialidade e integridade dos dados dos pacientes, em conformidade com requisitos legais aplicáveis.

Há que proteger a privacidade de um paciente e este tem de confiar na organização onde é tratado e onde confia a guarda dos seus dados pessoais.

3 ESTUDO DE UM CASO: SISTEMA DE INFORMAÇÃO CLÍNICA NO SNS

3.1. Introdução

Este capítulo irá incidir na análise dos aspectos críticos de segurança do registo clínico electrónico do paciente, identificados no Capítulo 2, no que concerne ao Serviço Nacional de Saúde (SNS) em Portugal. Serão abrangidos dois tipos de instituição responsáveis pela origem dos registos clínicos de pacientes: os hospitais e os centros de saúde.

A análise é baseada na experiência profissional e pessoal da autora com os sistemas de informação existentes no SNS, em contactos com outros profissionais da área e no estudo da documentação devidamente referenciada.

Os registos clínicos electrónicos surgem da necessidade crescente de estruturar e tornar acessível a informação clínica. Os primeiros dados clínicos a serem estruturados e informatizados foram os diagnósticos, os procedimentos e os resultados de exames laboratoriais.

O registo clínico electrónico do paciente e a sua partilha entre todos os profissionais envolvidos é essencial para a optimização dos processos de prestação de cuidados de saúde. No entanto, para que o registo e circulação da informação clínica seja bem aceite, é fundamental assegurar que se usem métodos fiáveis e seguros.

É importante conseguir um bom compromisso entre dois objectivos que por vezes entram em conflito: melhorar os cuidados de saúde prestados ao paciente e garantir a sua privacidade, integridade e disponibilidade dos dados.

Na grande maioria dos hospitais, a espinha dorsal do sistema de registo clínico electrónico é constituído pela aplicação SONHO[44], que interage com outras aplicações. No caso dos centros de saúde este papel é desempenhado pela aplicação SINUS[45]. Estas duas aplicações surgiram no final da década de 80 para satisfazer as necessidades organizativas no SNS[46] e a sua utilização está amplamente disseminada em Portugal.

---

[44] SONHO – Sistema Integrado de Informação Hospitalar.

[45] SINUS – Sistema de Informação para Unidades de Saúde.

[46] SNS – Sistema Nacional de Saúde.

O SONHO é um sistema integrado de informação desenvolvido pelo IGIF que abrange alguns departamentos (ou áreas de actividade) dos hospitais, tais como: urgência, consulta externa, internamento, arquivo clínico, meios complementares de diagnóstico. O seu principal objectivo é o controlo do fluxo de doentes dentro da organização. É uma aplicação essencialmente administrativa, modular e flexível e, em termos estruturais, tem condições para englobar novos módulos, interagir com outras aplicações (por exemplo, aplicações para gestão de laboratórios) e efectuar comunicações inter-institucionais (por exemplo, receber a marcação remota de consultas).

O sistema de informação SINUS, também desenvolvido pelo IGIF[47] [59], tem como objectivo suportar as actividades diárias dos centros de saúde. É constituído por vários módulos que implementam algumas funcionalidades (por exemplo, registo de utentes, agendas de consultas, registo de vacinação, cartão do utente).

A necessidade de criar um registo clínico electrónico levou o IGIF a desenvolver um módulo orientado à actividade do médico, o SAM[48], e um módulo orientado para a actividade de enfermagem, o SAPE[49]. Estes dois sistemas têm por base a informação clínico-administrativa processada no SONHO ou no SINUS. Uma vez que estes são sistemas diferentes, na realidade foram desenvolvidos dois módulos do SAM e dois módulos do SAPE: uma para os cuidados de saúde primários, integrado no SINUS; outro para os cuidados de saúde secundários, integrado no SONHO.

Cada um destes módulos tem por objectivo organizar e estruturar a informação registada no SONHO e no SINUS segundo uma perspectiva clínica no sentido de promover a qualidade da assistência prestada ao paciente.

As principais funcionalidades disponibilizadas pelo SAM nos Hospitais, permitem ao médico: efectuar o registo do diário da consulta, internamento ou urgência; prescrever meios complementares de diagnóstico e terapêutica; prescrever medicamentos; marcar próxima consulta; consultar e registar antecedentes pessoais e familiares; elaborar e consultar relatórios; aceder à "história clínica" do paciente; etc.

De salientar a funcionalidade do Processo Clínico Electrónico que tem vindo a ser implementada pelo SAM e que permite consultar informação detalhada sobre o paciente.

O SAM para os cuidados de saúde primários apresenta apenas a opção "Consulta Externa", que permite ao médico efectuar registos diários da consulta, prescrever medicamentos, marcar nova consulta (no centro de saúde ou remotamente no Hospital), aceder a informação sobre vacinação,

---

[47] IGIF – Instituto Gestão Informática e Financeira da Saúde.

[48] SAM – Sistema de Apoio ao Médico.

[49] SAPE – Sistema de Apoio à Prática de Enfermagem.

aceder à opção "Processo Clínico" do utente no centro de saúde e do Hospital, aceder a consultas de telemedicina e prescrever "Certificados de Incapacidade Temporária".

O IGIF em conjunto com a escola de enfermagem do Hospital de S. João desenvolveu dois módulos do SAPE, um orientado para a actividade do enfermeiro nos cuidados de saúde secundários (integrado no SONHO); outro, orientado para a actividade do enfermeiro nos cuidados de saúde primários (integrado no SINUS). O módulo integrado com o SONHO partilha principalmente dados relativos à identificação e internamento, enquanto que o módulo integrado com o SINUS partilha dados relativos à identificação e vacinação. Ambos pretendem ser uma ferramenta de apoio à actividade diária do enfermeiro, tendo por base a CIPE (ver Anexo A).

As principais funcionalidades disponibilizadas pelo SAPE nos hospitais permitem ao enfermeiro: registar intervenções que resultam das prescrições médicas; registar dados resultantes da avaliação inicial de enfermagem; registar fenómenos/intervenções de enfermagem; criar o plano de trabalho; etc.

As funcionalidades disponibilizadas pelo SAPE nos centros de saúde são muito semelhantes às existentes no SAPE dos hospitais. Permitem ao enfermeiro registar intervenções que resultam das prescrições médicas; registar fenómenos/intervenções de enfermagem; criar o plano de trabalho, entre outras.

A utilização destes módulos quer nos hospitais, quer nos centros de saúde, não está disseminada. A aplicação SAM em alguns hospitais é utilizada como registo clínico electrónico departamental e não hospitalar.

Na Figura 5 podemos observar de uma forma global as principais aplicações de registo clínico existentes no SNS, infra-estruturas de rede e principais fluxos de informação interinstitucionais.

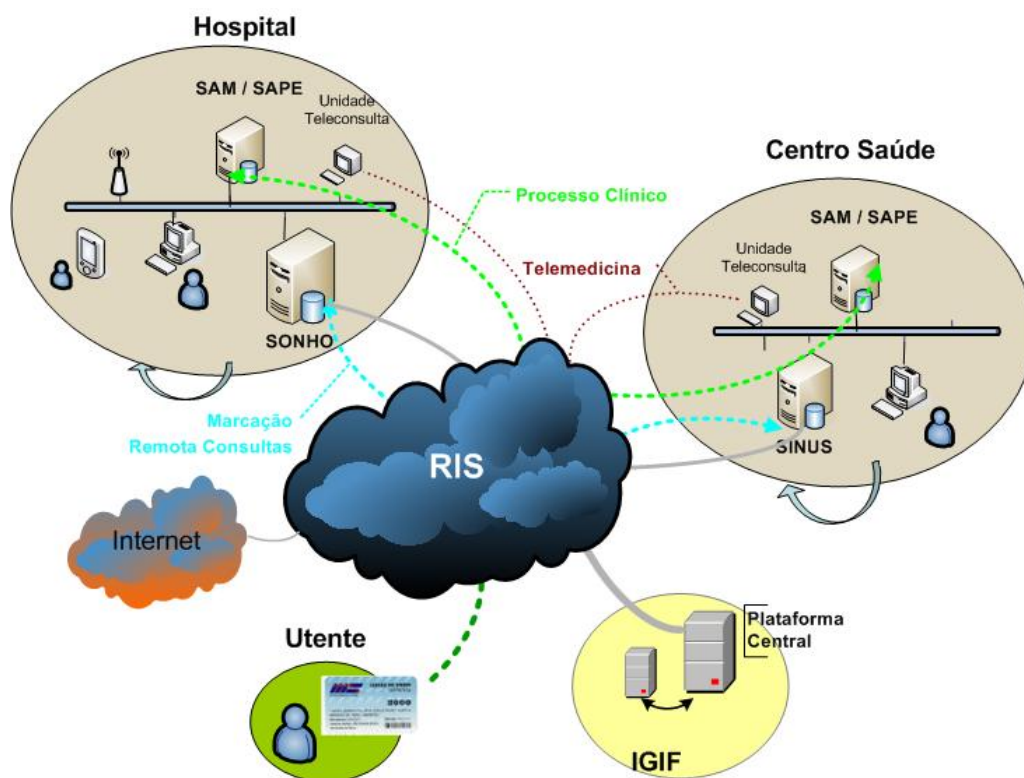



Figura 5 – Modelo do Sistema de Informação do Serviço Nacional de Saúde

Para facilitar o acesso aos cuidados de saúde foi criado o “Cartão do Utente”, sendo o IGIF a entidade responsável pela sua gestão. Permite identificar cada cidadão perante o SNS e outras entidades de forma inequívoca.

As comunicações inter-institucionais são realizadas através da RIS e, numa visão mais alargada, através da Internet. A RIS, constituída e gerida pelo IGIF, é uma rede multimédia de telecomunicações privada do MS[50] interligando as diversas redes locais das instituições, as quais por sua vez, interligam internamente os computadores de cada instituição.

A RIS apresenta-se actualmente como uma das maiores redes do país, abrangendo dentro do território continental os serviços centrais do MS, os hospitais e centros hospitalares do SNS e respectivas dependências, as administrações regionais de saúde e respectivas sub-regiões de saúde, os Centros de Saúde e extensões e os organismos autónomos e suas delegações.

De seguida será efectuada uma análise dos aspectos críticos de segurança identificados no Capítulo 2 nas aplicações e infra-estruturas de rede agora referidas.

[50] MS – Ministério da Saúde.

3.2. Desenvolvimento e Implementação

O sistema de registo clínico anteriormente referido, desenvolvido pelo IGIF, abrange diferentes áreas da prestação de cuidados de saúde. Fundamentalmente, o sistema é caracterizado por aplicações baseadas em sessão terminal tipo *telnet*, o caso do SONHO e do SINUS, e por aplicações mais recentes que usam tecnologias *web*, o caso do SAM e do SAPE. Para além destas aplicações, o sistema de registo clínico também poderá estar suportado por aplicações baseadas em arquitectura cliente-servidor (por exemplo, aplicações para gestão de laboratórios).

O SONHO e o SINUS usam bases de dados relacionais e estruturadas, que tipicamente são instaladas em servidores com sistema operativo *Unix*, usam um sistema de gestão de bases de dados *Oracle* e são desenvolvidas com ferramentas (*Forms 3.0, PL/SQL e Reports 2.0)*. Disponibilizam uma *interface* não gráfica (i.é., tipo terminal alfanumérico) para os utilizadores.

Embora o SONHO e SINUS usem bases de dados robustas e estruturadas, devido à sua antiguidade e arquitectura, são aplicações orientadas para funcionar em ambientes fechados e não estão conformes aos padrões internacionais que promovem a interoperabilidade dos sistemas, razão que dificulta a sua integração com outras aplicações (por exemplo, aplicações para gestão de laboratórios de análises clínicas). Para além disto, acresce o facto de que existem diferentes versões instaladas nas instituições, o que dificulta a sua gestão e manutenção por parte do IGIF e das próprias instituições. Tipicamente, também não existe uma configuração ou parametrização uniformizada entre as diferentes instituições, o que mais dificulta o trabalho da tutela, por exemplo, comparação de indicadores de gestão e ou produção.

As aplicações SAM e SAPE, suportadas na estrutura de base de dados do SONHO e do SINUS, foram desenvolvidas em ambiente *web* e apresentam uma *interface* amigável para o utilizador. No seu desenvolvimento foram incluídos tecnologia JAVA[51] e usadas ferramentas de desenvolvimento *Oracle Developer*. Tanto o SAM como o SAPE tipicamente estão instalados em servidores com o sistema operativo *Windows 2000 Server*.

Numa perspectiva mais técnica, o acesso às aplicações SAM e SAPE é suportado por um navegador (*browser*), e realizado por *applets* JAVA que estabelecem via JBDC[52] conexão com o sistema de gestão de bases de dados do SONHO ou SINUS.

---

[51] JAVA – O JAVA é uma linguagem de programação orientada ao objecto.

[52] JDBC – Java Database Connectivity.

Estes dois módulos estão desenvolvidos para funcionar em equipamentos móveis e rede sem fios, nomeadamente *Tablet PC* (o caso do SAM), e PDA (caso do SAPE na execução do "Plano de Trabalho de Enfermagem"). O recurso a estas tecnologias permite ao médico ou enfermeiro efectuar consultas ou registos junto à cama do doente.

O facto de estar a ser usada tecnologia *web* torna a distribuição e uso das aplicações bastante fácil, contribuindo para uma melhor portabilidade do sistema.

Podemos observar na Figura 6 um esquema da arquitectura de um sistema de informação clínico electrónico típico na grande maioria das instituições em Portugal. Numa perspectiva de integração, o processo clínico electrónico é um componente do SAM que centraliza em si toda a informação clínica do paciente de uma forma estruturada, sendo construído de uma forma aberta e de molde a receber informação de múltiplas aplicações que suportam o sistema.

Outras aplicações que suportam o sistema de registo clínico interligam com o sistema central (SONHO ou SINUS), e são importantes do ponto de vista da informação clínica (por exemplo, aplicações para registo de resultado de análises ou exames e arquivo de imagem médica). No entanto, não estão largamente disseminadas nas instituições e existe uma grande diversidade de soluções implementadas em diferentes plataformas, sendo por isso referidas genericamente como fonte de registos clínicos. Para além disto, geralmente estas aplicações apresentam um nível baixo de integração com a base de dados do SONHO ou SINUS podendo resumir-se apenas à importação da identificação do paciente.

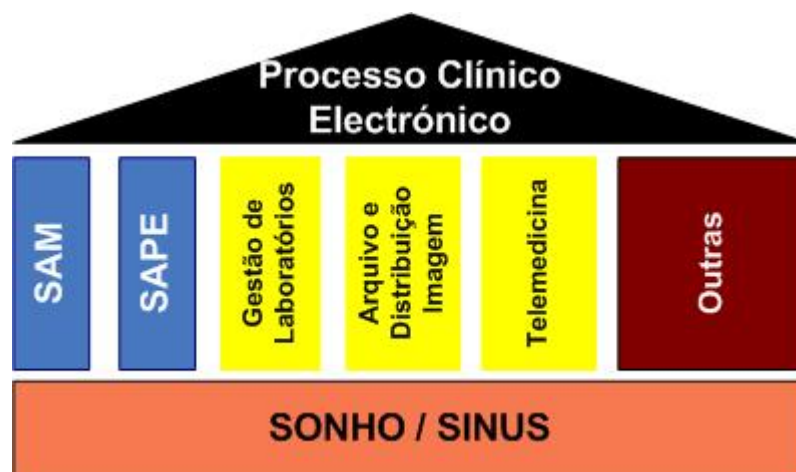



Figura 6 – Arquitectura do sistema de registo clínico electrónico

O sistema de registos referido suporta funcionalidades que permitem a partilha de informação entre diferentes instituições (por exemplo, marcação remota de consultas, acesso ao processo clínico ou sessões de teleconsulta) e, neste caso, a linha entre os utilizadores internos e os externos da rede

não está muito bem definida, pelo que aumentam as preocupações relacionadas com a segurança. As instituições confiam mutuamente em que a informação será mantida confidencial e que será usada com o propósito inicialmente estabelecido.

Devido à sensibilidade da informação e à heterogeneidade deste sistema, torna-se necessário um elevado nível de protecção e segurança e, nessa medida, foi considerado desde o início uma estrutura muito bem definida de controlo de acessos associados a uma estrutura que define o perfil e privilégios do utilizador nas diversas aplicações que integram o sistema de registo clínico.

No contexto do sistema de registos clínicos apresentado, o uso de uma linguagem classificada e a codificação da informação clínica estão directamente relacionadas com compreensão e integridade dos dados clínicos. Pela sua relevância, serão referidos alguns dos sistemas de classificação e codificação referidos no Capítulo 2 e detalhados no Anexo A: o ICD-9 na classificação da doença em diagnósticos ou procedimentos, o ICPC-2 na classificação internacional de cuidados primários, e a CIPE na classificação das práticas de enfermagem. A informação gerada de acordo com o ICD-9 representa uma apreciável fonte de elementos para análises, estudos estatísticos.

Por outro lado, o uso de estruturas de dados comuns e protocolos de comunicação permitem a interoperabilidade e a troca de dados entre diferentes sistemas (por exemplo, sistemas de arquivo e distribuição de imagem médica) ou mesmo instituições (por exemplo, sistemas de telemedicina). Para além disto, podem evitar fragmentação e redundância da informação e fornecer melhor qualidade dos sistemas de informação de saúde. Por esta razão, o sistema aqui descrito deveria ser repensado em conformidade com padrões reconhecidos internacionalmente (ver Anexo A), nomeadamente o HL7 no que se refere à interoperabilidade entre módulos ou sistemas, e o mais recente padrão de segurança HIPAA no que se relaciona com a implementação de políticas e procedimentos que garantam a privacidade da informação.

3.3. Identificação e Autenticação

O processo de identificação e autenticação usado pelo sistema de informação referido anteriormente traduz-se no uso do número mecanográfico para a identificação dos utilizadores, que é um número único de funcionário relacionado com a instituição. A autenticação é realizada através da inserção de uma senha. Para além disto, quando o médico é admitido pela Ordem dos Médicos em Portugal é-lhe atribuído um número único, o qual é inserido na estrutura base do sistema SONHO-SINUS, o que permite rastrear toda a actividade clínica do médico dentro da instituição.

O processo de autenticação no SONHO-SINUS baseia-se em algo que o utilizador sabe (por exemplo, uma senha), desde logo um mecanismo simples e fraco de controlo de acesso, para além de que é frequente a sua partilha. No entanto, disponibiliza diferentes níveis de acesso ao sistema.

No caso do SONHO e SINUS, que funciona em ambiente alfanumérico e UNIX, assim que utilizador entra no sistema UNIX usando a sua conta, é automaticamente direccionado para a aplicação onde não há autenticação adicional. Por exemplo, os mecanismos de autenticação tradicionais no *Unix* (caso do SONHO e SINUS) baseiam-se no *UserID*, no *Primary GroupID* e no *Secundary GroupID* a que o utilizador é associado. Quando um utilizador fornece o nome-utilizador/senha para acesso ao sistema *Unix*, a transmissão da senha é enviada em claro (por telnet, rcp[53] ou ftp[54]). O serviço que corre no servidor, por exemplo, o *"telnetd"*, vai pesquisar no ficheiro (/etc/passwd) pela entrada que contém aquele utilizador, de seguida procede à encriptação da senha fornecida pelo utilizador remoto e compara-a com a senha cifrada que se encontra armazenada no sistema (/etc/passwd, /etc/shadow). Se ambas coincidir dá-se a autenticação do utilizador. Como o utilizador faz parte de um grupo principal e de grupos secundários, irá ser invocada uma *shell* que tem como proprietária aquele *UserID* e atribuídos os respectivos privilégios.

O tamanho da senha não é limitado a um tamanho mínimo, no entanto deverá ser usado um número mínimo de caracteres ou existe a possibilidade de os utilizadores usarem senhas muito pequenas e previsíveis. Tipicamente não é definida uma data de validade da senha, que force o utilizador a alterá-la, no entanto os utilizadores têm a possibilidade de a alterar em qualquer altura.

Outro aspecto importante é o facto de o sistema não limitar o número de tentativas de conexão, o que facilita a ameaça de ataque por "força bruta" (várias tentativas até encontrar a senha correcta), especialmente quando a senha é previsível e pequena, e fácil de adivinhar, portanto.

É importante também referir que os administradores do sistema (por exemplo, profissionais de informática) em geral não possuem mecanismos de autenticação adicionais em relação aos outros utilizadores, no entanto, possuem um perfil de acesso diferente.

Para além destas questões, outro dos grandes problemas de segurança deste sistema é o facto de que não existe nenhum testemunho de acesso pessoal e intransmissível e que impossibilite o abandono do terminal com a sessão aberta.

Este tipo de identificação é usado em qualquer terminal remoto independentemente de estar a ser usado num ambiente crítico ou não. No entanto, no domínio dos sistemas de informação clínica críticos deveria ser usado a combinação de um ou mais mecanismos de autenticação: em que o utilizador sabe uma senha (por exemplo, senha para o SONHO), tem um testemunho (por exemplo,

---

[53] rpc – Remote Procedure Call. Chamada de um procedimento remoto. RFC 1057.

[54] ftp – File Transfer Protocol. Protocolo de transferência de ficheiros. RFC 959.

um cartão inteligente para assinatura digital ou certificados digitais) e é reconhecido por característica própria (por exemplo, íris, impressão digital, timbre vocal). Para maior comodidade dos utilizadores, a combinação do segundo processo com o terceiro, permitiria a autenticação do utilizador com algo que ele tem e algo que ele é, sem ter de se lembrar de senhas. Para além de que não seria possível partilhar as suas credenciais com outros profissionais.

Outro aspecto de segurança importante está no acesso ao sistema de registo clínico. O acesso às diversas plataformas não está centralizado e uniformizado. Basicamente em cada aplicação são criados os utilizadores e atribuídos os respectivos privilégios.

Uma possível solução poderá passar pela construção de uma plataforma segura de acesso único às aplicações, permitindo o *"Single Sign On"*, eventualmente com recurso à chave pública do utilizador. O utilizador possuiria um cartão onde está armazenado o seu certificado digital e a sua chave privada protegidos por senha. Quando o utilizador pretendesse aceder ao sistema centralizado apenas teria de estar na posse do seu cartão e facultar a senha. O nome de utilizador junto com o seu certificado digital serão enviados ao servidor a que pretende aceder.

No acesso à sala de servidores, poderiam existir mecanismos de identificação e autenticação ou não (dependendo da instituição), mas, no caso desta autenticação ser requerida, poder-se-ia processar em dois passos: algo que o utilizador tem (por exemplo, cartão magnético ou cartão de identificação profissional) e algo que o utilizador sabe (por exemplo, uma senha). Para além disto, os servidores deveriam estar alojados em armários fechados à chave e só alguns utilizadores específicos estar autorizados a aceder-lhes.

Finalmente, como foi dito anteriormente, o paciente utiliza o seu "Cartão do Utente" para interagir com o sistema. O cartão identifica o utente através de um código de barras e de uma banda magnética que contém informação sobre a morada, idade, naturalidade, nacionalidade, região de saúde e centro de saúde de residência do utente, subsistema de saúde e existência ou não de regime especial de comparticipação de medicamentos, entre outros elementos. No entanto, não existe qualquer mecanismo de protecção dos dados contidos no cartão. O "Cartão do Cidadão"ainda em fase experimental irá substituir, entre outros documentos, o "Cartão do Utente", trata-se de um documento dotado de características de segurança que irá permitir ao utente interagir com as entidades prestadoras de cuidados de saúde (ver Capítulo 4).

3.4. Controlo de Acessos

Como já foi referido, o controlo de acesso medeia a interacção entre os utilizadores e o sistema. Existe a necessidade de definir o perfil de utilizador e a que tipos de informação têm acesso.

Pela sua importância na tarefa de introdução de dados no sistema, classificação e codificação, os principais intervenientes neste sistema são essencialmente quatro: médicos, administrativos, enfermagem e os técnicos de meios complementares de diagnóstico e terapêutica. Para além destes, os profissionais de informática possuem um papel importante no controlo do sistema. Os investigadores são os elementos menos activos no sistema, no entanto possuem um papel muito importante nos resultados e no tratamento dos dados recolhidos pelos diferentes profissionais.

Como podemos ver na Tabela 2, é definido a que tipo de informação cada grupo profissional de utilizadores têm acesso, i.e., quem têm acesso e a quê.

Tabela 2 – Mapeamento utilizador/acção (conforme perfis pré-definidos na aplicação)

Grupo Profissional	Privilégios de acesso ao sistema
Médicos	Acedem ao módulo SAM e têm permissões para inserir, alterar ou eliminar os seus próprios registos médicos (por exemplo, prescrição de uma terapêutica ou medicação). Além disto, podem visualizar, mas não manipular os registos efectuados por outros médicos ou grupos profissionais (por exemplo, registos relacionados com resultados de exames ou análises clínicas). Acresce ainda o facto de lhes ser permitido classificar a informação clínica de acordo com os diagnósticos ou procedimentos clínicos realizados.
Enfermeiros	Acedem ao módulo SAPE e têm permissões para inserir, alterar e eliminar registos relacionados com os cuidados de enfermagem. Os utilizadores apenas podem aceder aos pacientes afectos ao departamento no qual estão a desempenhar funções. Além disto, podem ainda visualizar as terapêuticas ou prescrições médicas de forma a incluí-las no seu plano de trabalho e, caso lhes seja permitido, podem visualizar os registos clínicos do paciente através da funcionalidade "Processo clínico Electrónico". Para além disso, é possível restringir ainda mais criando sub-perfis com permissões, por exemplo, só para visualizar registos de enfermagem.
Administrativos	Os administrativos podem inserir e alterar (mas não eliminar) informação relacionada com a identificação do paciente. São responsáveis pela inserção ou alteração de toda a informação administrativa relacionada com os vários contactos do paciente com a instituição (por exemplo, marcação de meios complementares de diagnóstico, agendamentos, admissão à urgência, etc.). Os utilizadores em geral não estão autorizados a eliminar registos (por exemplo, termos de responsabilidade ou números de processo). Esta funcionalidade apenas está disponível aos gestores do sistema ou aos gestores departamentais (por exemplo, eliminar episódios de urgência). É vedado qualquer tipo de acesso aos registos médicos ou de enfermagem. Geralmente usam o SONHO-SINUS, podendo já ter acesso a alguns perfis administrativos no SAM na realização de algumas tarefas, nomeadamente no agendamento do bloco operatório.

Técnicos de MCDT[55]	Este grupo de utilizadores apenas está autorizado a aceder ao módulo da aplicação para gestão de MCDT no perfil para técnicos. Têm permissões para inserir, remover e alterar informação relacionada com o resultado de exames ou análises antes de serem validados pelo médico da especialidade.
Investigadores	Este grupo de utilizadores apenas está autorizado a aceder a um conjunto de informação clínica muito restrito (por exemplo: diagnósticos e procedimentos médicos por idade ou sexo). Geralmente os dados para análise são disponibilizados pelos profissionais de informática. No sistema, tipicamente apenas possuem privilégios para visualizar alguma informação.
Informáticos	Têm acesso ao sistema com perfil de gestor permitindo-lhe executar tarefas de manutenção (por exemplo, gerir utilizadores e cópias de segurança). Apenas eles tem acesso à base de dados de forma a executar pesquisas directamente nas tabelas, com o intuito de corrigir alguns problemas (repôr a consistência ou integridade dos dados), de facilitar a investigação médica ou eliminar informação redundante relacionada com os pacientes. No entanto, por exemplo, o acesso aos dados clínicos via módulo do SAM ou SAPE é-lhes restringido.

Como podemos observar na tabela anterior, os diferentes grupos profissionais possuem diferentes níveis de privilégios no acesso e manipulação da informação clínica. Mesmo dentro do mesmo grupo de utilizadores (por exemplo, administrativos), existem diferentes perfis de acesso de acordo com as suas funções ou departamento no qual se integram. Por exemplo, um utilizador que desempenha funções na área da consulta externa poderá ter acesso ao perfil de consulta, mas mesmo dentro do perfil podem ainda existir sub-níveis (ou restrições) configurados de acordo com as funções desempenhadas.

Como foi anteriormente referido, para além da fragilidade do mecanismo de identificação e autenticação usado, baseado no par nome-utilizador/senha e senhas previsíveis, um dos grandes problemas identificados e que pode comprometer seriamente a segurança do sistema é o facto de existir uma grande mobilidade de utilizadores (por exemplo, administrativos) por períodos de tempo curtos, pelo que é difícil a manutenção do seu perfil de acesso, o que leva a que, partilham entre si o acesso ao sistema. Outro factor é, por não terem o necessário conhecimento das funções dos diferentes perfis, estes poderem intencionalmente ou por descuido modificar informação e comprometer a integridade dos dados. No entanto, sempre que possível, os utilizadores recebem formação ou informação orientada às funções a desempenhar. Uma boa política é permitir ao utilizador acesso apenas àquilo que ele precisa para realizar o seu trabalho e nada mais. Por vezes é importante que ele desconheça outras funcionalidades ou privilégios, o que poderá ser um obstáculo a possíveis ataques.

[55] MCDT – Meios Complementares de Diagnóstico e Terapêutica.

Para além dos aspectos referidos, acresce ainda o facto de que, na generalidade das instituições, não existe uma protecção entre a rede da instituição e a base de dados ou aplicações. Qualquer utilizador não autorizado pode tentar aceder ao sistema através da rede, podendo ter a tarefa facilitada com a ajuda das ferramentas certas. Deveria existir uma *firewall* protegendo o tráfego entre estes dois pontos.

Outro aspecto extremamente importante é o controlo dos acessos provenientes do exterior à rede local da instituição (por exemplo, IGIF, centros de saúde ou empresas de manutenção remota). São utilizadores autorizados, logo devem ser alvo dos mesmos cuidados de segurança que os acesso provenientes da rede interna. Por exemplo, no acesso à base de dados do SONHO é usado um mecanismo de controlo de acesso simples e fraco, baseado no binómio nome-utilizador / senha que circula em claro pela rede. Neste caso, dever-se-ia recorrer ao uso do um protocolo de comunicação seguro (por exemplo, SSH) no estabelecimento de um canal seguro para transporte dos dados clínicos entre o utilizador externo e a instituição.

O sistema usa uma identificação única do paciente, designado por número do processo clínico do paciente. Associado e este número de processo, e por cada contacto que o paciente tem com a instituição, é gerado um número de episódio (por exemplo, um episodio de urgência, internamento ou consulta). Relacionado com cada episódio poderão estar associados outros dados (por exemplo, prescrições e meios complementares de diagnóstico e terapêutica). Este processo de identificação permite rastrear registos na base de dados relacionados com o paciente, para além de facilitar a realização de auditorias, o controlo de acessos e a manutenção da integridade da base de dados. Este método de identificação permite realizar pesquisas à base de dados com fins estatísticos ou de investigação, evitando que os pacientes sejam identificados directamente.

Em situações de emergência em que não é possível identificar o paciente, o sistema gera um episódio de urgência ao qual os utilizadores podem associar registos e fica à espera que lhe chegue mais informação relacionada com a identificação do paciente. Esta medida permite que não haja perda de dados importantes e seja mantida a consistência da base de dados.

Outra questão muito importante é facto de que não existe identificação única a nível nacional do paciente. À medida que o paciente se dirige a uma instituição ou organização de prestação de cuidados de saúde vai sendo gerado uma identificação local, e assim a história clínica do paciente fica espalhada pelas diferentes instituições ou organizações.

Finalmente, o paciente tem o direito de aceder à sua própria informação ou pelo menos definir quem tem acesso e a que tipo de informação. Actualmente, os sistemas de registo clínico electrónico a funcionar na maioria das instituições que integram o MS não implementam esta funcionalidade. Está previsto que venha a ser possível através do portal da saúde aceder a informação clínica pessoal mediante a identificação do paciente pelo “Cartão do Cidadão” (ver

Capítulo 4). No entanto este tipo de acessos deve apenas permitir a consulta dos registos sem que seja possível alterá-los, de outra forma iria comprometer a integridade da sua informação clínica. Contudo, o paciente tem o direito de saber quem acedeu à sua informação clínica e negar acessos, e assim impedir que a sua informação "caia" em mãos não autorizadas (por exemplo, seguradoras).

3.5. Monitorização, Auditoria e Logs

Como foi referido no Capítulo 2, os *logs* permitem auditar ou rastrear o acesso à informação podendo constituir um forte dissuasor a tentativas de abuso ou de acesso não autorizado à informação clínica do paciente. Para evitar alguns dos problemas de segurança mais comuns com os *logs*, eles devem ser feitos e analisados regularmente para que a maior parte das acções dentro do sistema possam ser monitorizadas e relatadas frequentemente, evitando desta forma que eventos não detectados (por exemplo, acessos não autorizados) passem completamente despercebidos.

Os *logs* registam detalhes sobre o acesso à informação incluindo a identidade do utilizador, perfil de acesso, data e hora, fonte e destino, informação pesquisada e retirada e, talvez, as razões do acesso àquela informação.

No sistema em análise há diferentes tipos de *logs*: os que são gerados pelo sistema operativo; os que são gerados pela base de dados; os que são gerados pelas aplicações. No se refere ao primeiro caso, quer para os acessos internos ou externos à rede da instituição, é registado a identificação do utilizador, identificação do acesso, identificação da máquina (nome ou endereço IP), data e hora do acesso e o tempo em que esteve conectado. Quanto aos *logs* gerados pelas aplicações: no SONHO-SINUS é registado o número mecanográfico, nome do utilizador, perfil de acesso, data e hora de entrada e saída na aplicação; no SAPE é registado a identificação do utilizador, data e hora de entrada e saída na aplicação, para além de que ao longo da sua utilização é possível visualizar quem foi o utilizador que inseriu ou deu termo aos registos de enfermagem; a aplicação SAM ainda não disponibiliza informação que permita auditar ou rastrear a actividade do médico, a não ser que se vá directamente às tabelas da base de dados. No entanto estes *logs* não registam detalhes da informação pesquisada, inserida ou modificada.

Estão implementados mecanismos de monitorização e alerta da base de dados baseados em sondas do tipo SMON (System Monitor) e PMON (Process Monitor). A SMON é responsável por monitorizar a actividade do sistema (por exemplo, sistema operativo ou da instância Oracle). No caso de falha da instância Oracle, este mecanismo permite a recuperação dos dados que não foram gravados. A PMON é responsável por fazer uma limpeza após a ocorrência de falhas em processos.

Os alertas são guardados num ficheiro em texto simples, a que os utilizadores autorizados podem aceder e comprometer a sua integridade sem serem detectados.

Outro aspecto importante é o facto de os *logs* serem armazenados no mesmo servidor da base de dados que estão a monitorizar. Os mecanismos de controlo de acesso aos *logs* são os mesmos que para aceder ao sistema à base de dados e às aplicações, não existindo protecções específicas no que se refere a esta informação.

Finalmente, são realizadas cópias de segurança regulares dos *logs* mas geralmente não são aplicados controlos de segurança adicionais, a não ser os procedimentos habituais de cópias de segurança.

3.6. Gestão de Base de Dados

Antes de definir o tipo de segurança a usar nos servidores é necessário saber que tipo de sistema de gestão de base de dados, sistema operativo e outro tipo de software é ou vai ser usado.

Como foi referido atrás, tipicamente o SONHO-SINUS é instalado em servidores com sistema operativo *Unix (Solaris)* e SGBD[56] *Oracle*. As aplicações SAM e SAPE, desenvolvidas em *Oracle Developer*, tipicamente encontram-se instaladas em servidores com sistema operativo *Windows Server 2000* e usam o SGBD do SONHO-SINUS.

A manutenção do sistema é partilhada pela equipa técnica do IGIF e pelos técnicos das instituições. Apenas estes têm acesso à base de dados de forma a executar pesquisas directamente nas tabelas, com o intuito de corrigir alguns problemas (repor a consistência ou integridade dos dados), facilitar a investigação médica ou eliminar informação redundante relacionada com os pacientes.

A versão do *Oracle* usado na implementação das aplicações SAM e SAPE possui algumas características apertadas de segurança (combina encriptação dos dados armazenados e durante a sua transmissão com mecanismos de autenticação forte) que fornecem confidencialidade aos dados, e também integridade. No entanto, os dados administrativos e clínicos do sistema são enviados e armazenados na base de dados do SONHO-SINUS), e este sistema de gestão de bases de dados não implementa qualquer mecanismo de segurança ou encriptação dos dados. Este aspecto é uma das principais vulnerabilidades do sistema.

---

[56] SGBD - Sistema de Gestão de Base de Dados.

Uma possível solução passaria pelo recurso a um mecanismo de segurança forte baseado no uso tecnologia de chave pública. Por exemplo, em cada servidor SONHO-SINUS deveria ser desenvolvido uma nova estrutura em que cada utilizador autorizado tivesse um certificado digital associado, emitido e assinado pelo servidor.

Por exemplo, esta nova estrutura passaria pelo uso do módulo PAM[57] [124] [125], que é um módulo centralizador do processo de autenticação usado pelo *Sun Solaris* e que permite o uso de certificados digitais. A principal vantagem do PAM, além de centralizar as funções do nome-utilizador/senha, é de ser capaz de seleccionar os programas aos quais os utilizadores têm acesso. Tipicamente as aplicações (login, telnet, ftpd, rlogin, dtlogin, su, passwd, ssh, e outros) estão incluídas neste módulo e as outras poderiam ser acrescentadas por simples configuração.

No servidor deveria ser incluída a chave pública de uma autoridade certificadora (ver discussão apresentada no Capítulo 2) em que o servidor iria reconhecer as credenciais dos utilizadores.

Outro aspecto muito importante é a validação dos dados introduzidos na base de dados e relacionados com o estado clínico do paciente. Por exemplo, o resultado mal inserido de uma análise pode ter consequências graves no tratamento do paciente. Deverão ser adoptadas políticas que conduzam à utilização de métodos de validação e correcção dos dados, de codificação e de parametrização de forma a minimizar situações de inconsistência. Para além de que periodicamente o sistema deverá ser auditado por alguém com conhecimentos clínicos de forma a validá-lo.

O sistema disponibiliza mecanismos que permitem realizar procedimentos regulares de cópias de segurança da base de dados a diferentes níveis: diário, semanal e mensal. Estes procedimentos são cruciais não só porque permitem recuperar o sistema no caso de ocorrer uma avaria ou um ataque, mas também fornecem informação de forma a repor a original. Estes procedimentos deveriam ser realizados de forma automática sempre que possível; no entanto, algumas destas fases ainda são executados de forma manual. Também seria desejável o uso de mecanismos criptográficos nos processos de cópias de segurança de forma a impedir o acesso (por exemplo, por parte do atacante) à informação nelas contida. Na realidade isto não acontece, pelo que, se um atacante tiver acesso às cópias de segurança, pode ficar a conhecer a informação recolhida durante anos pela instituição. Felizmente, as instituições possuem algumas preocupações de segurança no que toca à destruição segura dos dados e na guarda das *tapes* de cópias de segurança em local adequado e devidamente protegido contra roubos ou deterioração.

---

[57] PAM – Pluggable Authentication Module.

Em termos de segurança física, a plataforma mais usada disponibiliza redundância de discos duros (discos em *mirror*). O programa de *mirror* duplica a informação nos discos (quer em termos de sistema operativo, base de dados ou aplicação) de maneira a que em caso de falha de um deles o sistema continue disponível através de outro. Também existem circuitos e equipamentos de UPS[58] que fornecem energia contínua e mantêm o sistema a funcionar em caso de cortes de corrente eléctrica. Estes circuitos poderão ainda estar apoiados por um sistema de "geradores de emergência", como é o caso em algumas instituições (por exemplo, hospitais). Outro aspecto importante, e que nem sempre se verifica, é a redundância de três peças essenciais: placa de rede, fonte de alimentação e processador. Se algumas destas peças falha o sistema fica indisponível até que estas sejam substituídas ou reparadas.

A segurança física deverá ser dimensionada não só de acordo com o equipamento a segurar, mas também de acordo com as necessidades dos utilizadores. Mesmo em sistemas considerados não críticos, a actividade dos profissionais de saúde depende da disponibilidade do sistema de informação clínico. Por exemplo, o acesso à história clínica de um paciente ou aos resultados de uma análise ou exame no momento certo pode resultar no melhor ou pior tratamento do paciente.

3.7. Gestão das Comunicações

3.7.1. Apresentação das infra-estruturas

Com já foi referido, os principais objectivos da RIS são interligar todas as redes das instituições do MS e disponibilizar um conjunto de serviços de rede como por exemplo: ligação à Internet; correio electrónico; marcação remota de consultas; acesso remoto a *data centers*; cartão do utente; telemanutenção de equipamento e software; acesso a bases de dados centrais; videoconferência; aplicações de telemedicina; integração do serviço de voz/dados e imagem na rede; etc.

A RIS apresenta uma arquitectura de sucessivos nós concentradores: genericamente, as extensões dos centros de saúde comunicam para as suas sedes; as sedes, comunicam para as respectivas sub-regiões; estas estão conectadas aos nós centrais do IGIF Porto, Coimbra e Lisboa, os quais, por sua vez, se concentram no nó de Lisboa. Os meios de interligação são alugados a operadores de telecomunicações como por exemplo, a Portugal Telecom e ONI. O IGIF é

---

[58] UPS – Unidade Ininterrupta de Alimentação.

responsável pela manutenção de toda a infra-estrutura até aos encaminhadores instalados nas instituições.

Com a reestruturação operada recentemente no triângulo Lisboa, Porto e Coimbra, e como referido anteriormente, a “espinha dorsal” da RIS apresenta-se em tecnologia ATM (ver Figura 7). A opção por esta tecnologia, deve-se principalmente, à necessidade de suporte integrado de voz, vídeo e dados em tempo real. Estes serviços requerem parâmetros de qualidade que normalmente não são necessários no tráfego normal de dados de aplicações do tipo base de dados.

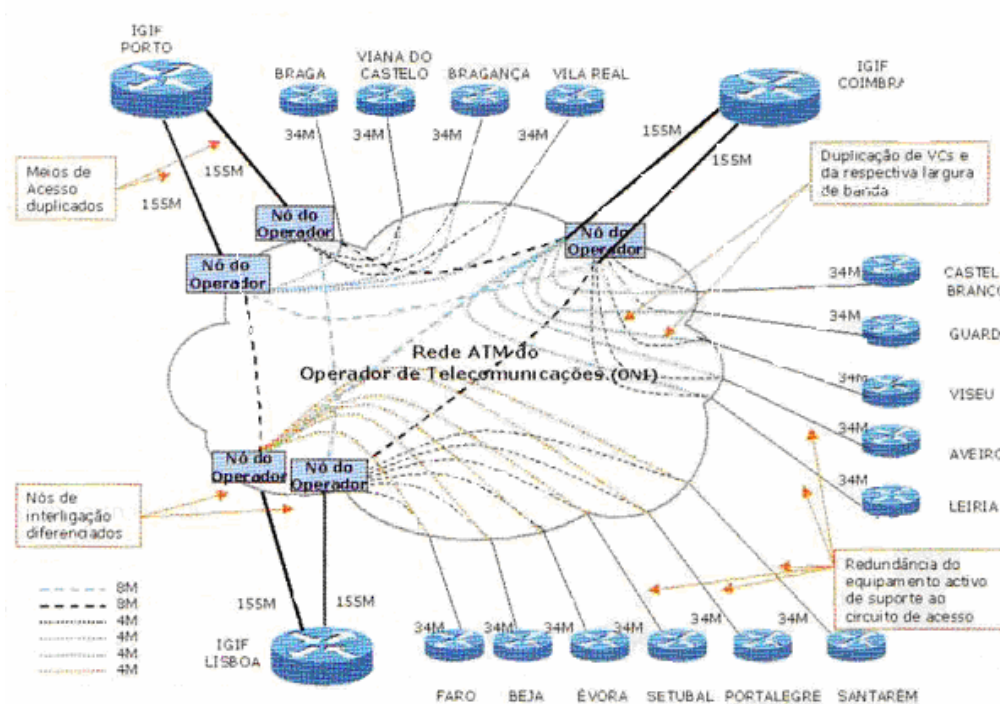



Figura 7 – Esquema Geral da “Espinha Dorsal” da RIS

(Fonte: Inter.face Nº77, Tecnologias da Informação no Sector da Saúde)

As ligações entre os pontos de concentração distritais e os pontos centrais da rede dão-se através de circuitos virtuais com larguras de banda que variam entre os 8Mbps e os 16Mbps com capacidade para evoluir até 34 Mbps nos distritais, e 155Mbps nos pontos centrais. O equipamento instalado permite evolução para ligações a *Gigabit*, quando tal se justificar. Entre os principais nós de acesso às capitais do distrito a rede está dotada de uma capacidade de 8Mbps, com sistemas de redundância do equipamento activo de suporte ao circuito de acesso.

As infra-estruturas de rede locais das instituições são do tipo *Ethernet*, cablagem estruturada, apresentam topologia em estrela e estão ligadas à RIS através de circuitos dedicados ou linhas RDIS (ver Figura 4).

3.7.2. Aquisição de dados, Transmissão e Gestão

Hoje em dia as redes de comunicação são constituídas por componentes semelhantes e tecnologias idênticas, pelo que possuem as mesmas ameaças e vulnerabilidades. Algumas das ameaças e vulnerabilidades, ou pelo menos as mais importante, já foram referidas no Capítulo 2 e poderão servir de listagem ao sistema em análise.

Assim, neste sub-capítulo, serão analisados aspectos de segurança das redes de comunicação que suportam o sistema. Como podemos observar na Figura 5, a informação circula na rede local da instituição, na RIS (por exemplo, marcação remota de consulta ou consulta de telemedicina) ou num âmbito mais alargado pela Internet (por exemplo, manutenção remota de equipamento ou software por empresas). Esta infra-estrutura baseia-se em tecnologias normalizadas como o TCP/IP na troca de informação.

Tipicamente as redes locais estão ligadas à RIS através de circuitos dedicados RDIS (com larguras de banda que variam entre 128Kbps a 2Mbps) protegidas por *firewall* ou por filtros de acesso implementados nos equipamentos de interligação (*routers*), como representado na Figura 8.

A ligação da RIS à Internet é efectuada em dois pontos de acesso, no Porto a 8Mbps em Lisboa a 16Mbps.

Em resumo, são de realçar as seguintes características da RIS: é uma infra-estrutura separada da Internet com defesa de perímetro (por um sistema de *firewall*); sistema de redundância em vários pontos; ferramentas de antivírus e AntiSPAM; conceito de gestão pró-activa; evolução dos requisitos de segurança; melhor gestão da largura de banda; monitorização e gestão em tempo real da rede e de tráfego; sistemas de *cache* inteligente distribuídos *(proxy)*; sistemas de classificação de tráfego com prioridade QoS (voz, dados, videoconferência e transmissão de informação clínica multimédia).

O IGIF é, responsável pela manutenção de toda a infra-estrutura até aos encaminhadores instalados nas instituições. A partir daqui as instituições são responsáveis pela gestão da sua infra-estrutura.

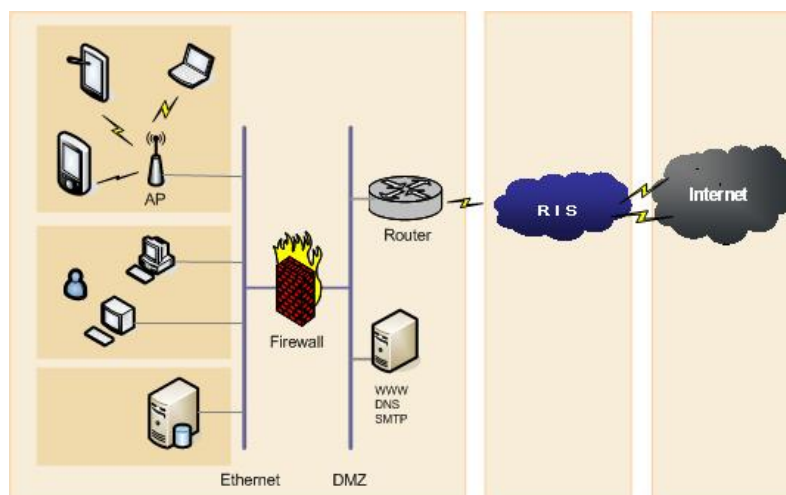



Figura 8 – Arquitectura da Infra-estrutura de Rede

Como já foi dito, as infra-estruturas de rede locais das instituições são do tipo *ethernet*, cablagem estruturada, topologia em estrela e estão ligadas à RIS através de um "*router*".

A distribuição aos utilizadores é feita por cabos em cobre com *switches* que disponibilizam portas *ethernet* a 10/100Mbps/1Gbps. Em geral os equipamentos de comutação possuem ligações redundantes em todos os bastidores locais ligados ao bastidor principal por fibra óptica a *Gigabit Ethernet*. A ligação da rede local à RIS é feita por circuito dedicado com largura de banda que varia entre 64 Kbps a 2Mbps. Em geral, também existe uma linha RDIS adicional instalada por motivos de segurança, sendo utilizadas em caso de falha do circuito dedicado.

Outro aspecto muito importante é que algumas instituições têm implementado redes sem fios integradas nas suas redes cabladas. O uso de redes sem fio na vertente clínica no que se refere à realização de teletrabalho e o acesso a dados clínicos através de terminais móveis (Tablet PC, Pocket PC, Telemóveis, etc.) levanta questões específicas relacionadas com a segurança e com a restrição do seu uso por parte de utilizadores não autorizados.

Tanto a *web* como o correio electrónico estão a tornar-se meios privilegiados na troca, aquisição e divulgação de informação clínica. A utilização destes meios pelos profissionais de saúde no que se refere ao acesso e troca de informação clínica do paciente envolve aspectos muito importantes relacionados com a segurança.

Os computadores ligados à rede local de cada instituição, para além de poderem estar ligados ao sistema de registo clínico, têm a possibilidade de ter acesso aos serviços de Internet e correio electrónico. Para além disto partilham a mesma rede onde circula informação relacionada com os pacientes. Embora exista um *firewall* que separa os servidores do sistema da rede exterior, o servidor de correio electrónico e internet localiza-se numa zona desmilitarizada DMZ e poderão surgir algumas ameaças sérias que poderão comprometer a segurança da informação do paciente. Para

minimizar esta ameaça, deveria ser implementado uma separação entre o tráfego com origem no exterior e o tráfego interno.

Além de tudo isto, no caso das instituições de saúde usarem serviço de correio electrónico na troca de mensagens com informação clínica associada, deveriam recorrer a mecanismos que garantam a segurança das mensagens. Tais mecanismos passariam pelo uso de técnicas criptográficas, por exemplo, aplicações de correio electrónico seguro PEM[59] e PGP e certificados digitais para troca de chaves públicas.

No caso de acesso remoto a bases de dados disponibilizadas pela RIS, por exemplo, SIGIC[60] ou à base de dados dos utentes (gestão do Cartão do Utente), a segurança destes serviços deverá estar condicionada ao uso de tecnologias como o SSL / HTTPS[61], associadas a técnicas de criptografia de dados, as quais permitem transacções seguras entre os navegadores e servidores *web*. Na RIS, existem servidores seguros que garantem elevados níveis de segurança, no que respeita à autenticidade e confidencialidade na troca de informação.

As ameaças e vulnerabilidades com as ligações ao exterior são muito importantes, mas as ligações internas não deverão ser minimizadas. O impacto de um ataque interno poderá ter consequências muito mais graves. As lacunas de segurança internas são mais difíceis de detectar e por isso de difícil resolução.

As comunicações são estabelecidas no modo cliente-servidor. Isto significa que todos os terminais de acesso às aplicações (por exemplo, SAM, SAPE ou SONHO-SINUS) podem aceder à informação armazenada no servidor. Entre cada cliente e o servidor existe a rede da instituição através da qual a informação flúi. Este aspecto poderá ser uma fonte de ameaças à segurança porque entre os utilizadores (clientes) e o servidor não existe nenhum mecanismo que impeça a tentativa de acessos não autorizados. Uma *firewall* deveria existir para filtrar e registar a informação circulante. Além disto, porque nem toda a informação circula encriptada (por exemplo, no SONHO e SINUS) durante todo o processo de comunicações entre o cliente e o servidor a escuta ilícita da informação em trânsito é uma importante ameaça à segurança. Pelo facto da informação circular em claro na rede é muito fácil capturar informação sensível relacionada com o utente e usá-la com um propósito diferente daquele para o qual estaria previsto.

---

[59]PEM - Privacy Enhancement Mail. Procedimentos para autenticação e encriptação de mensagens. Para mais especificações ver, RFC1421, 1422, 1423 e 1424.

[60] SIGC – Sistema Integrado de Gestão de Inscritos para Cirúrgica. Programa do governo Português para gerir as listas de espera para cirurgia.

[61] SHTTP - Secure Hypertext Transfer Protocol. Protocolo HTTP suportado por SSL. Especificações no RFC 2660.

A informação que circula entre os postos clientes do SAM - SAPE e o servidor aplicacional e de base de dados é encriptada através de mecanismos de segurança implementados pela própria tecnologia de desenvolvimento das aplicações. Os servidores aplicacionais SAM e SAPE estão conectados ao servidor de base de dados do SONHO ou SINUS, como já foi referido. Na grande parte das instituições estes constituem a base de dados central da informação clínica do paciente.

Existem diversas ferramentas disponíveis na Internet (por exemplo, *etherreal*) que poderão em muito ajudar o atacante.

A encriptação da informação clínica é muito importante, mesmo dentro da rede interna da instituição, porque esta circula por diferentes locais aonde utilizadores não autorizados têm acesso e, como já foi referido, os utilizadores com acesso à rede interna representam uma das principais vulnerabilidades de segurança.

Alguns mecanismos de segurança tais como SSL, SSH ou IPsec descritos anteriormente são algumas opções a implementar. O SSL poderá ser um dos protocolos a usar para manter a segurança do canal de transmissão entre clientes e servidores baseados em tecnologia *web*.

Outro aspecto importante é a aquisição remota de informação através da integração de consultas de telemedicina, marcação remota de consultas e acesso ao processo clínico do paciente no sistema. As comunicações inter-institucionais estabelecem-se através da RIS, e usam os mecanismos de segurança que as próprias aplicações implementam ou outros que possam ser implementadas adicionalmente. Por exemplo, numa marcação remota de consulta entre o SINUS e o SONHO a informação transita na rede às claras. No entanto, por exemplo, numa consulta de telemedicina ou acesso ao processo clínico do paciente baseado no uso de tecnologias *web*, a informação poderá circular em canal protegido ou encriptada.

Aquisição remota de informação clínica na casa do paciente não está ainda considerada neste sistema.

Os aspectos de segurança, ameaças e vulnerabilidades relacionados com a aquisição de informação com origem externa à instituição são basicamente as anteriormente referidas. No entanto serão relevados alguns aspectos de segurança que deverão ser considerados na aquisição remota de informação, como por exemplo: no que se refere à autenticação do utilizador externo nome-utilizador/senha deverá ter uma referência diferenciada da dos utilizadores internos; a *firewall* e o processo de auditoria do sistema deverão registar todos os acessos externos tal como registam os internos, para poderem ser analisados; as comunicações deverão ser encriptadas para todos os tipos de dados, por exemplo, o uso de VPNs e IPsec; formação dos novos utilizadores para o uso do sistema de registo clínico é um procedimento muito importante; revisão das políticas de segurança.

O IGIF disponibiliza às várias instituições que integram a RIS ligações do tipo VPN para apoio remoto, entre as empresas (por exemplo, fornecedores de equipamentos, aplicações ou

comunicações) e as instituições. Embora este tipo de acesso seja disponibilizado a pedido, poderá representar uma ameaça à segurança caso a sua gestão e controlo não seja adequado.

Ainda no que se refere às intervenções de manutenção remota, por exemplo uma transferência de ficheiros ou sessão remota poderá basear-se nos protocolos *telnet* ou *ftp* que são inseguros, pois toda a informação passa de forma transparente e às claras na rede, permitindo a captura de informação confidencial incluindo credenciais de autenticação nome-utilizador/senha dos servidores das várias instituições. É recomendável o uso de mecanismos capazes de garantir sessões seguras, por exemplo mecanismo com base no protocolo SSH.

Para além de todas estas questões, deverão ainda ser consideradas: actualizações de segurança do software e alterações à topologia da rede. Um conhecimento do ambiente em que opera, das pessoas e tecnologias é a melhor forma de cobrir todos os aspectos relacionados com a segurança do sistema e, ao mesmo tempo, saber como reagir no caso de este não funcionar como o esperado.

3.8. Conformidade com Ética, Legislação e Normas

Aspectos éticos ou códigos de conduta estão implícitos na utilização do sistema de registo clínico electrónico. Como foi dito no Capítulo 2 (ponto 2.8), em Portugal a CNPD apoia a elaboração de códigos de conduta no artigo 32º, como refere a Lei 67/98 de 26 de Outubro para a Protecção de Dados Pessoais. A presente lei é relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

È muito importante que a informação clínica armazenada pelo sistema em análise esteja abrangida por esta legislação. Relativamente às obrigações definidas pela CNPD, é de referir que os sistemas em análise foram objecto de registo na CNPD. Relativamente à aplicação de sanções, é importante que sejam definidas responsabilidades caso ocorra algum evento que possa colocar em risco a informação.

Para além de tudo isto, e no contexto da RIS, o IGIF elaborou um conjunto de normas ou regulamento de utilização da RIS tendo em vista regular algumas questões de segurança relacionadas com a rede, serviços e os seus intervenientes, a seguir referidos.

Para eventuais ataques internos o IGIF refere no artigo 5º – Suspensão do Serviço de Rede, alínea 5.1, “ (…) suspender (…) serviço de rede a um utilizador, desde que esteja a interferir no normal funcionamento de toda ou parte da RIS, (…) tentativas de intrusões não autorizadas em sistemas alheios e de uso indevido da infra-estrutura nacional”.

O mesmo regulamento e relativamente a ataques externos, diz no artigo 7º – Segurança, alínea 7.1, refere “ (…). O IGIF compromete-se a pôr em prática normas de segurança contra

tentativas de intrusão com origem na Internet, não se responsabilizando, no entanto por tentativas de intrusão originadas em instituições integradas na RIS. (…)".

Nas ligações da RIS a outras entidades não integradas nesta infra-estrutura, o regulamento prevê, artigo 11º – A RIS e as Outras Redes ou Entidades, alínea 11.1, "As ligações a outras instituições ou redes não integradas na RIS têm que ser solicitadas ao IGIF (…) pondo em prática as medidas de segurança tidas por convenientes".

É de referir o "Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais" realizado pela CNPD aos Hospitais em 2004 [93], que retrata o estado actual dos sistemas de informação na saúde em Portugal. Algumas das conclusões desse relatório, mostram que a "Lei da Protecção de Dados Pessoais" não é suficiente para garantir a segurança e confidencialidade dos dados pessoais. Nesse documento foi dada particular atenção às aplicações que interagem com o médico, no que toca ao respeito pela privacidade dos pacientes (por vezes não usam qualquer mecanismo de autenticação, não fazem separação lógica entre dados administrativos e de saúde, etc.), e no que afecta a integridade dos dados (por vezes não são feitas cópias de segurança ou não existe suporte alternativo em caso de perda acidental dos dados), etc.

As grandes conclusões resultantes da análise do relatório merecem ser aqui resumidas: cerca de 50% das instituições não informa a CNPD do tratamento de dados pessoais dos pacientes; na generalidade, não é obtido "consentimento informado" dos pacientes para a recolha e tratamento dos dados pessoais; verifica-se um generalizado incumprimento da lei no que diz respeito à utilização dos dados clínicos em investigação científica (pedido de autorização à CNPD para este tipo de utilização).

Também ficou claro que, pelo facto do processo clínico também se encontrar em suporte papel, por mais esforços que sejam feitos, existem riscos de a informação clínica ficar acessível a pessoal não autorizado. A CNPD considera que só a automatização do processo clínico dotado das necessárias medidas de segurança (senhas, perfis de utilizadores e separação lógica entre dados administrativos e lógicos) podem conferir confidencialidade à informação clínica dos pacientes.

Em conclusão, existe a preocupação de aplicar normas e legislação de segurança adequada a este tipo de sistema de informação; no entanto, a maior parte refere-se apenas ao uso de informação electrónica. Em Portugal não existe legislação específica na área da segurança para ambientes de prestação de cuidados de saúde, muito menos para o registo clínico electrónico do paciente, tal como existe o HIPAA nos EUA (ver Capítulo 2). Contudo, existe legislação portuguesa que regulamenta os direitos à privacidade e o acesso à informação clínica, mas que não é muito concreta relativamente à informação a que se pode aceder ou não. É urgente definir regulamentação específica relacionada com os dados pessoais do paciente.

3.9. Grelha de Avaliação de Aspectos de Segurança

Para demonstrar a aplicabilidade da grelha referida no Capítulo 2, no âmbito dos sistemas de informação para a saúde, irá ser aplicada ao sistema de registo clínico SONHO, em uso numa grande parte hospitais públicos em Portugal. É apenas uma exemplo que espelha a realidade em algumas instituições.

Pela análise resumida da grelha (ver Tabela 3), podemos avaliar o SONHO como um sistema que carece de algumas melhorias em termos de segurança, nomeadamente no reforço de segurança ao nível da autenticação do utilizador e na segurança dos dados que circulam na rede. Ao nível da utilização, é necessário criar uma interface com o utilizador mais amigável, pois a actual complexidade é uma potencial ameaça à integridade dos dados.

Ao nível de administração do sistema, conviria dispor-se de procedimentos eficazes de administração local e remota, de criação de cópias de segurança e de mecanismos de controlo de acessos.

Tabela 3 – Grelha de Avaliação dos Aspectos de Segurança do SONHO

Avaliação dos aspectos de segurança (exemplos de questões): SONHO							Legenda: 1-Fraco; 2-Insuficiente; 3-Razoável; 4- Bom; NA-Não Aplicável; NS-Não Sei
Aspectos a Avaliar	**Avaliação**						**Justificação**
	1	**2**	**3**	**4**	**NA**	**NS**	
Autenticação e Autorização dos utilizadores							
São utilizados mecanismos de autenticação por tipo de utilizador (administrador, utilizador, gestor, etc)? Quais são?			x				O mesmo mecanismo de autenticação / identificação nome/senha para os diferentes tipos de utilizadores. São usados perfis de utilização.
Existem políticas de senhas? São alteradas regularmente?		x					Senha do sistema alterada regularmente. A senha dos utilizadores não.
São dadas e controladas as permissões por tipo de utilizador?			x				São usados perfis por tipo de utilizador e área profissional.
Confidencialidade dos dados							
Existem mecanismos de garantia de confidencialidade no acesso aos dados em operação normal?			x				Existem diferentes níveis de acesso aos dados em função do tipo de utilizador e perfil.
E em situação de ataque? Os mecanismos de protecção são suficientemente robustos?						x	Não são conhecidos mecanismos de protecção (p.ex: algoritmos de cifra).
E no caso de acesso aos dados para estudos estatísticos ou científicos?			x				É criado perfil adequado com acesso restrito.
Integridade dos dados							
Existem mecanismos que permitam controlar a integridade dos dados em operação normal?			x				Servidor com discos em *mirror* , fonte alimentação e placa de rede redundante. Ar condicionado. Acesso restrito à sala de sistemas. São efectuadas diferentes tipos de cópias de segurança (diário, semanal e mensal). É desconhecida a existência de outros mecanismos.
E em situação de ataque? Os mecanismos de protecção são suficientemente robustos?	x						Os dados são armazenados em "claro".
Existe procedimentos de verificação, correcção e controlo de qualidade dos dados?			x				São desenvolvidos *scripts* em SQL para controlo de qualidade dos dados. Não fazem a verificação da sua alteração.
Disponibilidade do sistema							
Existem mecanismos para garantir a disponibilidade do sistema em operação normal?			x				Servidor com discos em *mirror* , FA e placa de rede redundante. Infraestrutura de rede com *links* em redundância e equipamento *switch* . No caso de falha de corrente eléctrica, existe UPS e gerador de emergência
Existe mecanismos para contrariar potenciais ataques ao sistema do tipo "Negação de Serviços"?						x	
Tolerância a falhas do sistema em caso de avaria? E em caso de ataque?			x				Servidor com discos em *mirror* . Processador, FA e placa de rede redundante. Em caso de o ataque, por exemplo, desligar o ar condicionado, o acesso à sala é condicionado.No caso de falha de corrente eléctrica, existe UPS e gerador de emergência
Existência de pontos críticos informáticos?		x					Base de Dados Oracle centralizada no mesmo servidor. Hardware redundante.
Existência de pontos críticos físicos?	x						Todos os sistemas redundantes estão na mesma sala.

Auditabilidade							
Existe registos que permitam efectuar auditoria?				x			Existe *logs* ao nível da BD, do SO e da aplicação.
Que informação é registada?				x			Ao nível da aplicação regista os eventos, acessos dos utilizadores. Ao nível do SO regista o acesso dos utilizadores (utilizador | identificação terminal | datas) e mensagens de erro / alerta. Ao nível do Oracle mantém *logs* dos *backups.*
Existe verificação regular desses registos?					x		Verificação manual de *logs* .
Que meios suportam esses registos?	x						Geralmente o próprio servidor. Cópias de Segurança.
Utilização ao nível de administração							
A administração do sistema é remota ou tem de ser feita na consola?					x		É possível administração remota a partir da rede local ou a partir da RIS (IGIF).
Quais os mecanismos de autenticação utilizados? Existem cuidados especiais?		x					Autenticação por nome / senha. Alteração periódica da senha de administração da BD e do gestor aplicacional.
De que forma é feita a protecção da sessão de administração remota?	x						Em geral não são utilizados mecanismos de protecção. É simplesmente utilizado um *telnet* .
Os procedimentos de administração estão documentados?	x						Documentação praticamente inexistente. Alguns procedimentos realizados internamente estão documentados, mas os procedimentos não estão uniformizador para todos os hospitais.
As interfaces são fáceis de perceber e utilizar?		x					O interface é em "modo texto" e, genericamente, é pouco amigável.
Em situação de elevada carga do sistema o administrador têm prioridade de acesso?	x						Em situação de sobrecarga o administrador não tem prioridade.
É possível configurar o sistema de diferentes formas, para diferentes utilizadores?			x				O sistema permite definir diferentes perfis de utilização e administração.
Que poderes tem o administrador? Existe diferentes tipos de administradores?		x					O administrador tem todos os poderes de administração do sistema, da BD e aplicacional. Não existem diferentes tipos de administrador.
Acessos ao sistema para estatística?		x					O acesso a informação para tratamento estatístico está disponível em diferentes perfis. No entanto é necessário tratar o aspecto da confidencialidade. O gestor da aplicação tem acesso por SQL a toda a estrutura da aplicação.
Utilização normal							
O acesso ao sistema é remoto ou local?		x					Acesso ao sistema é via rede (remoto). É usado emulador de terminal "Reflection".
A utilização do sistema está devidamente documentada?	x						Documentação de utilização do sistema praticamente inexistente.
Mecanismos de autenticação utilizados?		x					Autenticação por nome / senha. Não existe mecanismo que obrigue o utilizador a alterar periodicamente a sua senha de acesso à aplicação.
As interfaces são fáceis de perceber e utilizar?		x					O interface é em "modo texto" e, genericamente, é pouco amigável.
Em situação de elevada carga do sistema?					x		Em situação de sobrecarga o acesso é lento e tentativas de conexão são descartadas.
Acessos ao sistema para estatística?			x				Acesso por perfil.
Conformidade com normas							
O sistema está em conformidade com certificações oficiais?					x		CNPD
Qual é o grau de conformidade?						x	Documentação insuficiente.

Mecanismos de defesa							
É usado algum sistema criptógrafico de protecção?	x						O SONHO não usa qualquer mecanismo criptográfico.
A que nível são usados os mecanismos criptográficos? (Ao nível aplicação, ao nível do sistema ou ao nível da rede?)						x	
Grau de robustez do sistema criptográfico? (Qual o algoritmo e o comprimento das chaves de cifra?)						x	
Existe mecanismos para prevenção de intrusão?		x					No servidor em geral não existe antivirus instalado. Antivirus nos postos de trabalho (actualizado diáriamente).
Existe mecanismos para detecção de intrusão?			x				No sistema está configurado uma sonda RMON e SMON.
Existe mecanismos de recuperação em situação de intrusão?						x	Se se tratar de uma recuperação após intrusão (ex. acção de um virus), provavelmente irão reinstalar o sistema e repor os dados afectados, usando as cópias de segurança)
Comunicações							
Tipos e meios de comunicação usados?			x				Rede Ethernet, RIS. São redundantes. Pode existir situações de rede sem fios.
Os meios usados são propícios a escuta e quebra de confidencialidade dos dados transmitidos?		x					A rede é constituida por tecnologia comutada em redundância. A informação circula em "claro". Os "ataques" podem ter origem dentro da instituição ou da RIS.
Existe mecanismo para garantir a integridade da informação em trânsito?	x						Não existe mecanismo para prevenir a escuta, alteração ou injecção. A informação circula em claro na rede.
Existe mecanismo de certificação do utilizador de forma a prevenir o "disfarce"? Qual?	x						Não existe mecanismo de certificação do utilizador. Apenas existe a autenticação inicial nome/senha.
Existe mecanismo para prevenir a interrupção das comunicações?			x				Existe redundância ao nível da LAN e na ligação à RIS.
Documentação							
Existe informação técnica para administração do sistema?		x					Documentação insuficiente nas instituições. A administração/ configuração é feita pelo IGIF.
Existe informação para a utilização do sistema?	x						Documentação insuficiente.

3.10. Conclusão

Em resumo, as estruturas do sistema alvo do estudo falham pela base pois desde logo são utilizados mecanismos simples e fracos de controlo de acesso, baseados no binómio “nome-utilizador/senha” que circula livremente pela rede, sendo frequente a partilha por colegas. Refere-se situações em que os utilizadores se levantam dos postos de trabalho e deixam as suas sessões abertas. A má prática do uso deste sistema compromete muitas vezes todo o processo, pelo que o aparecimento de mecanismos de autenticação fortes e de controlo destas práticas (auditorias e agentes de segurança activos) é imprescindível para o sucesso de um bom sistema de registo clínico. A implementação de mecanismos que forneçam uma autenticação forte baseada em testemunhos seguros é, pois, imperativa. Uma solução com requisitos mínimos pode passar, por exemplo, por se exigir a utilização de mecanismos de chave pública e cartões inteligentes protegidos por código. Adicionalmente, e subindo a complexidade, pode recorrer-se, para sectores de informação mais sensíveis, a mecanismos de informação biométrica (por exemplo, impressão digital). Deve dizer-se que estas tecnologias são já relativamente acessíveis mas, apesar disso, em Portugal não são implementadas na esmagadora maioria dos sistemas de registo clínico.

É urgente que as instituições criem regras e uma política de acessos com critérios na atribuição de acessos e perfis do utilizador; revisão regular dos acessos; mudança regular da chave de acessos; mecanismos que impeçam que o utilizador deixe a sua sessão aberta quando abandona o posto de trabalho; auditoria; etc.

A implementação de mecanismos de segurança passa pelo recurso a técnicas criptográficas de forma a providenciarem fortes garantias de confiança nos sistemas, mas também exige uma prática institucional e social adequada.

4 TENDÊNCIAS E TECNOLOGIAS EMERGENTES

4.1. Introdução

Neste capítulo será referido um conjunto de tendências no domínio das infra-estruturas e dos sistemas e informação clínicos e tecnologias na saúde. As principais tendências referidas são: integração dos sistemas de informação e dos dados clínicos intra ou inter unidades de saúde público-privadas ou outros parceiros; mobilidade dos sistemas de informação, profissionais de saúde e pacientes (por exemplo, a telemonitorização); acesso dos pacientes aos sistemas de informação, (informação geral de saúde e serviços *online*: o caso de marcação de consultas); voz sobre IP através da RIS; uso de cartão profissional e de cidadão; normalização.

Esta análise é baseada na experiência e observação profissional e pessoal da autora, contactos com outros profissionais da área e análise de documentação devidamente referenciada.

Nas próximas secções ir-se-á apresentar o que de maior relevo ou impacto para o futuro de saúde em Portugal está a emergir no que toca a tecnologias baseadas na informática. Alguns dos pontos referidos irão ser tratados em detalhe posteriormente outros não.

4.1.1. Integração dos Sistemas de Informação Clínica

Na perspectiva do desenvolvimento de uma sociedade da informação, cada vez mais se torna relevante uma nova estratégia integradora e agregadora dos sistemas de informação clínica focalizados no cidadão. A cada utente do SNS deverá estar associado um número único do processo clínico electrónico como núcleo de todo um sistema, o qual se deverá basear fundamentalmente nos seguintes princípios: registos únicos e individuais; movimentação da informação e não do utente; respeito pelos princípios de segurança e confidencialidade de informação nos registos.

Torna-se assim claro, a necessidade urgente de haver uma política nacional e integrada de sistemas de informação e comunicações na saúde, a qual deverá forçosamente passar por uma integração de sistemas, baseada numa agregação das soluções já existentes. Tal implicará a adopção de uma solução única a nível nacional e o mais normalizada possível, em função das melhores práticas internacionais, especialmente no espaço europeu.

Esta reformulação da política para os sistemas de informação na saúde poderá não obrigar à adopção de aplicações comuns a todas as instituições, o que implicaria migrações de soluções normalmente trabalhosas e penosas, mas antes constituir uma infra-estrutura nacional que permitisse a interacção e integração de todas essas aplicações.

Tal estratégia passaria por tirar partido do já criado “Data Center” da Saúde, alojado no IGIF, interligando e integrando as diversas unidades de saúde públicas e privadas, transaccionando de forma segura a informação dos pacientes e disponibilizando-a através de interface *web* onde e quando necessária.

4.1.2. Portal da Saúde

Conforme o preconizado pelo plano de acções do eEurope 2005 [98] [99] “Uma sociedade de informação para todos”, no ponto, “Redes de Informação de Saúde”, os estados membros devem desenvolver redes de informação de saúde nos pontos de prestação de cuidados de saúde (hospitais, laboratórios, centros de saúde, e até aos lares da 3ª idade) com conectividade em banda larga, quando adequado.

Seguramente, uma estratégia deste tipo, desde que devidamente sustentada por parcerias público-privadas, com viabilidade técnica e financeira, elevaria todo o sector da saúde em Portugal em termos de qualidade, eficácia e eficiência na prestação de cuidados de saúde.

A existência desta rede, com o recurso à Internet e o acesso do paciente a partir de casa, potenciaria diversas soluções de “HomeCare”, obviamente suportadas à distância pelos prestadores de cuidados de saúde. Como a Internet é cada vez mais utilizada pelo cidadão, poderia utilizada para fornecer mais informações médicas; neste contexto era fundamental que os conteúdos e serviços de saúde em linha fossem desenvolvidos de modo eficiente, estivessem disponíveis para todos. E que as páginas *web* ligadas à saúde obedecessem a critérios de qualidade estabelecidos (por exemplo, ao HON Code e eHealth Code (ver Capítulo 2)). Como exemplo, o ministério da saúde disponibilizaria informação de saúde genérica ao cidadão através do portal da saúde [97]. Com esta iniciativa, poder-se-ia implementar, por exemplo, o pedido de marcação de consultas on-line e o acesso à informação clínica pessoal. O acesso ao portal seria livre, por http ou fortemente protegido com mecanismos de autenticação forte (por exemplo, https) no que se refere à obtenção de informações pessoais.

4.1.3. Cartão do Cidadão

Uma das medidas propostas, no âmbito do eEurope 2005, visa o uso de cartões de saúde electrónicos na identificação única do paciente e sua interacção com o sistema de saúde. Nesta medida, o governo português está a promover o “Cartão do Cidadão” [111] [112]. É um documento único que irá agregar o bilhete de identidade, cartão do contribuinte, o cartão de utente do serviço nacional de saúde, cartão de beneficiário da segurança social e o cartão de eleitor. Este documento, ainda em fase de testes, permitirá a identificação e autenticação do cidadão perante serviços

informatizados da administração pública em Portugal, inclusive, a interacção de forma segura com os diferentes serviços de prestação de cuidados de saúde. Tudo isto com garantias de segurança física que dificultam usurpação de identidade e que impossibilitem a violação da privacidade do cidadão, impedindo o acesso a quaisquer dos seus dados pessoais sem o seu consentimento expresso.

O cartão do cidadão possui um "chip" que conterá certificados digitais (para autenticação e assinatura electrónica) podendo vir a conter outros dados, designadamente dados de saúde. Por aqui se vê a importância de existir uma infra-estrutura de chaves públicas à escala nacional.

Alguns dos objectivos mais importantes deste plano de acção passam pela instalação progressiva de uma infra-estrutura segura da informação e de uma abordagem comum de arquitectura de registos electrónicos de saúde através da normalização e intercâmbio de boas prática relativas a outras eventuais características funcionais, como dados de emergências médicas e acesso seguro aos dados de saúde pessoais. Foram já adoptadas algumas medidas neste domínio a nível da UE: directiva relativa à protecção dos dados pessoais no sector das telecomunicações; criação de uma unidade para a cibersegurança; adopção, pelos sectores privados e públicos, de uma cultura da segurança na concepção e na aplicação dos produtos de informação e comunicação; comunicações seguras entre serviços públicos.

4.1.4. Telemedicina

Por fim, mas não menos importante, refira-se outra das acções propostas pelo eEurope, a telemedicina. A telemedicina tornou-se um elemento fundamental da política sanitária aos níveis regional, nacional e europeu. São do conhecimento público alguns casos de sucesso em Portugal, alguns em fase de consolidação dos seus objectivos e integrados na rede informática da saúde (RIS), nomeadamente: a rede de telemedicina do Norte, o projecto CALENO [133] que promove a telemedicina em Castela e Leão e o Nordeste Transmontano; o projecto de telemedicina da região centro, do qual se destaca a teleconsulta em cardiologia pediátrica que envolve o Hospital Pediátrico de Coimbra [132]; o projecto de telemedicina da região alentejana [136], entre os 5 hospitais da região e centros de saúde; o projecto de telemedicina no Algarve [136].

Algumas das especialidades da telemedicina emergentes poderão vir a revolucionar a forma de prestar cuidados de saúde em Portugal, por exemplo: a telemedicina em emergência médica ou pré-hospitalar [103], que já foi alvo de algumas experiências pelo Instituto Nacional de Emergência Médica, (realização no local do acidente de um electrocardiograma e subsequente envio a um centro de orientação de doentes urgentes para análise por um especialista); a realização remota de intervenções cirúrgicas (telecirurgia) [104] com a utilização de manipuladores, robots e videoconferência avançada (por exemplo, cirurgia laparoscópica); o envio de sinais biológicos,

imagens médicas, dados laboratoriais desde o local do paciente a um centro especializado de monitorização (telemonitorização).

4.1.5. Normalização

Conforme referido no Capítulo 2 e em detalhe no Anexo A, no domínio da normalização em Portugal as tendências mais importantes são: a implementação do padrão HIPAA, no que se relaciona com a privacidade dos registos médicos dos pacientes; a adopção da norma HL7, no que respeita a troca, manutenção e integração de dados relativos a pacientes; o adopção da norma ISO/WD 27799, no que refere à gestão da segurança na área da saúde; e, ao nível da interoperabilidade dos sistemas de saúde, a adopção da norma ISO/TR 16056 (Interoperability of telehealth systems and networks).

Os dados de saúde são especialmente delicados, pelo que todas as acções neste domínio devem ser acompanhadas pelo desenvolvimento dos meios técnicos e organizativos que garantam a protecção dos dados pessoais contra o acesso, a divulgação e a manipulação não autorizados.

4.2. Sistema de Informação Clínica Integrado

No âmbito do “Plano Estratégico de Sistemas de Informação” para o SNS (Serviço Nacional de Saúde), através do projecto “Sistema de Informação Integrado da Prestação de Cuidados de Saúde” o IGIF pretende dar uma nova abordagem às tecnologias de informação e comunicação para a saúde. Os princípios básicos deste plano são: multiplicidade nas formas de acesso; oferta integrada de serviços; solução padronizada; plataforma integradora; gestão e exploração centralizada das tecnologias de informação e comunicação.

4.2.1. O Data Center da Saúde

As aplicações SONHO e SINUS desenvolvidas sobre uma plataforma descontinuada, representam no contexto actual de necessidade de partilha de informação um risco para as instituições. O IGIF pretende na sua estratégia criar um sistema de informação integrado de prestação de cuidados de saúde (ver Figura 9), estando já em curso o processo na área dos cuidados de saúde primários, a evoluir posteriormente para a área hospitalar.

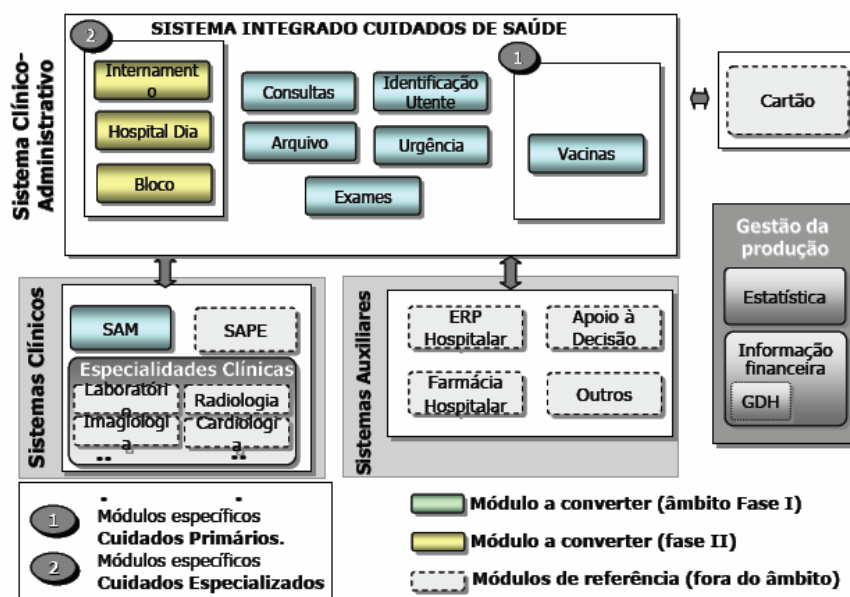



Figura 9 – Sistema Integrado de Cuidados de Saúde

(Fonte: Sistema Integrado de Gestão da Prestação de Cuidados de Saúde, IGIF)

Nesta nova arquitectura, em desenvolvimento, os utilizadores acedem ao sistema através de qualquer dispositivo equipado com um navegador *web*. Este sistema será composto por diferentes tipos de servidores (servidor *web*, servidor de aplicações ou componentes e servidor de base de dados). Os serviços poderão ser disponibilizados por máquinas diferentes, ou estar reunidos numa única máquina. Este sistema será suportado pela infra-estrutura da rede informática da saúde.

No que se refere ao armazenamento de dados, o que está em causa, é a escolha entre um cenário centralizado (com servidores num ou mais *data centers*) ou um cenário distribuído (com servidores em cada instituição).

Uma decisão nesta matéria passa necessariamente por uma análise de custos e benefícios detalhada. Aparentemente uma solução do tipo *data center* terá mais vantagens para hospitais e centros de saúde de reduzida dimensão do que para hospitais de grande dimensão.

Na realidade, os avanços tecnológicos têm mostrado uma tendência (ver Figura 10) para a disseminação ou globalização do acesso (via *web*, por diferentes canais de comunicação, redes com ou sem fios, dispositivos móveis, etc.) e a concentração de dados, serviços e aplicações (localizadas em *data centers* ligados entre si através de canais de muito alto débito).

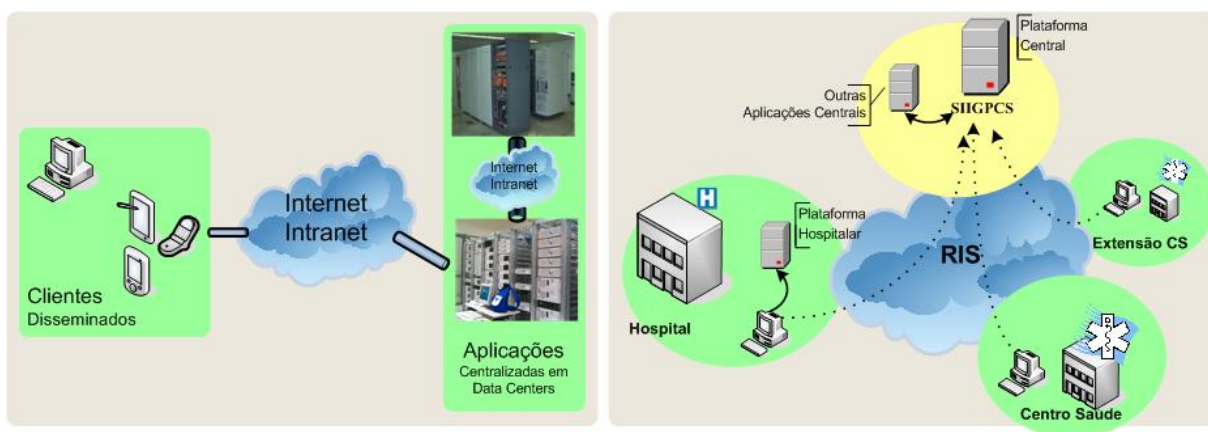
Um sistema deste tipo deverá assegurar elevada qualidade dos serviços prestados e acesso e partilha controlada de informação e serviços.

a) Globalização do acesso *b) Concentração de dados*

Figura 10 – Data Center da Saúde

As soluções baseadas em *data center* ou descentralizados apresentam alguns problemas relacionados com a segurança da própria arquitectura, a salientar os custos com fiabilidade e segurança das comunicações, que são necessariamente acrescidos pois tem de se dar mais atenção a mecanismos de redundância e à maior qualidade dos equipamentos e programas. Por outro lado as soluções centralizadas têm como inconvenientes o maior impacto de falhas no servidor ou ataques ao servidor, pois afecta um maior número de utilizadores (no limite todos os utilizadores podem ser afectados) e a dificuldade de protecção da propriedade e privacidade, porque informação sensível do ponto de vista da privacidade dos pacientes (dados clínicos) e do ponto de vista do valor patrimonial (para as unidades de saúde) vai estar fisicamente concentrada.

Para além destes aspectos críticos aumentam as preocupações relacionadas com a segurança na circulação da informação clínica e a necessidade de controlo de acessos e protecção. Aumenta também a vulnerabilidade a ataques de intercepção das comunicações e escuta ilícita da informação em trânsito.

Para além da existência de mecanismos que garantam a disponibilidade e confidencialidade da informação clínica, também é muito importante a existência de mecanismos que garantam a sua integridade. Para garantir a integridade dos registos clínicos é necessário, por exemplo, garantir o controlo de erros de introdução ou alterações não autorizadas dos dados e a segurança nas comunicações.

4.2.2. O Processo Clínico Electrónico Integrado Multimédia

Com o processo clínico electrónico único pretende-se criar um sistema de informação integrado do processo clínico electrónico em que a identificação do utente é única a nível nacional e até internacional, e onde se pode ter interoperabilidade entre os diferentes organismos de saúde

(hospitais, centros de saúde, lares, consultórios particulares, farmácias, laboratórios, pacientes, etc.) transaccionando de forma segura a informação dos pacientes e disponibilizando-a onde e quando for necessária.

Pretende-se que seja um sistema de interface amigável de suporte à actividade dos profissionais de saúde e que represente um ponto único de acesso ao sistema de informação clínica em Portugal (por exemplo, através do "Portal da Saúde").

Um dos possíveis cenários seria a centralização dos registos clínicos do paciente numa base de dados nacional (ou uma por região, numa primeira fase) que contivesse os dados sobre a informação clínica que os pacientes vão gerando à medida que efectuam contactos nas diferentes instituições de saúde (ver Figura 11), quer do sector público, quer do sector privado.

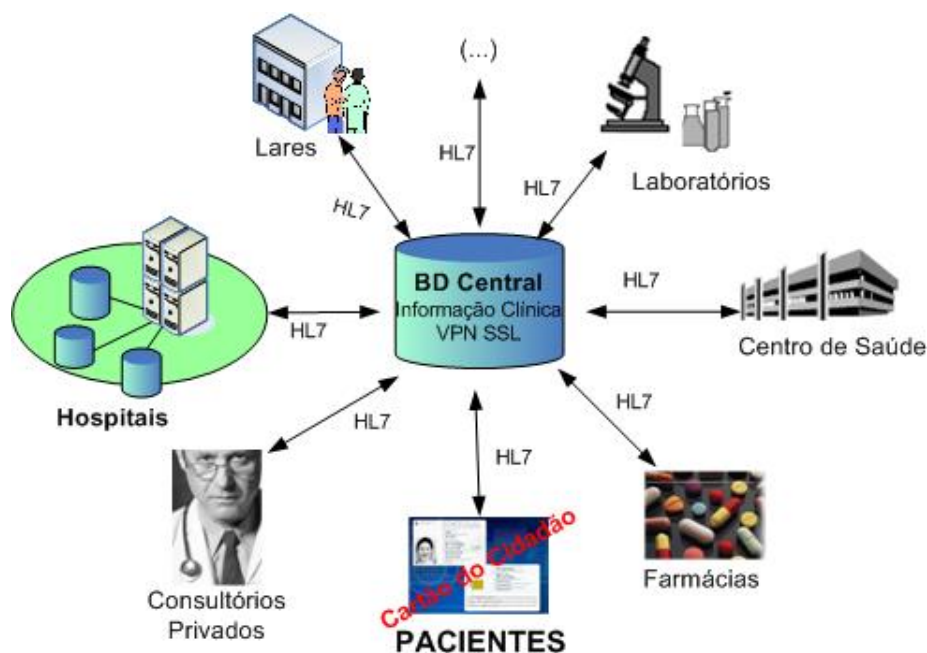



Figura 11 – Centralização do Registo Electrónico do Paciente

Por sua vez, as instituições que prestam estes cuidados (pelo menos hospitais e centros de saúde) deveriam ter acesso a esta base de dados para dois tipos de actividade: actualização, introdução de dados de forma automática à medida que a informação clínica sobre os pacientes é recolhida localmente; e consulta, por parte dos profissionais de saúde no momento em que estão a prestar cuidados aos pacientes.

É claro que esta base de dados central deveria estar alojada num local bem equipado em termos de infra-estruturas, controlo de acessos e mecanismos de tolerâncias a falhas, ou seja, num *data center* (como anteriormente referido) que respeite estes e outros requisitos.

Também os sistemas locais teriam de estar integrados com a base de dados central para que a informação clínica a ser centralizada (duplicada ou apenas referida por um mecanismo de apontadores para as bases de dados locais) estivesse em conformidade com a norma HL7.

As organizações ou pessoas que não integram a rede informática da saúde, deverão recorrer a ligações do tipo VPN ou SSL no acesso ao sistema central de informação clínica.

O acesso seguro aos registos clínicos do paciente (em situações normais de prestação de cuidados de saúde) deverá ocorrer em duas fases. Numa primeira fase, os profissionais de saúde deverão usar o seu cartão de identificação profissional (ver ponto 5.1 do Capítulo 5) na interacção com o sistema de informação. Numa segunda fase, deverá ser obtido o consentimento do paciente (através do cartão do cidadão) de acesso aos dados pessoais.

Para tudo isto ser possível é imprescindível o uso de uma estrutura de interfaces e terminologias comuns (por exemplo, conformidade com a norma HL7) e consenso internacional sobre segurança (por exemplo, implementação de uma infra-estrutura de chaves públicas).

Em Portugal, um exemplo inovador no desenvolvimento de uma nova geração do processo clínico electrónico é o projecto RTS (Rede Telemática da Saúde) [82].

Ainda em fase de desenvolvimento o projecto RTS consiste na interligação regional de instituições prestadoras de cuidados de saúde. Preconiza o projecto e implementação dos alicerces de uma rede, bem como de um conjunto de serviços telemáticos com o intuito de agilizar a cadeia de valor e diminuir os custos na prestação de cuidados de saúde à população da região de Aveiro. A RTS baseia-se num modelo de sucesso desenvolvido na Dinamarca e projecta o desenvolvimento de uma nova geração de processo clínico electrónico. Os principais objectivos do projecto são a partilha de informação clínica entre instituições e a construção de um "Portal Regional de Saúde".

O portal regional de saúde assenta em duas vertentes: a *área utente*, com acesso a informações genéricas sobre saúde e, mediante autenticação, a serviços básicos geridos pela RTS e ficha clínica pessoal; a *área reservada* a profissionais de saúde, com disponibilização de informação clínica permanente, actualizada e íntegra, para partilha entre as várias instituições envolvidas.

Do "Relatório de Análise de Processos e Fluxos de Informação" [82] [83], realça-se os seguintes os serviços prioritários a disponibilizar: no caso dos profissionais de saúde, sistema seguro de autorizações e certificações electrónicas, acesso a resumos de episódios de prestação de cuidados, partilha de documentos digitais e notas clínicas; no caso do utente, gestão da "minha saúde" (agenda de saúde, pedidos de marcações ou renovação de receituário, etc.), e gestão de conta corrente de saúde.

Do mesmo relatório podemos observar a definição de serviços piloto orientados para a obtenção dos resultados pretendidos. O piloto 1 - Serviços Telemáticos Infraestruturais, relacionado com os aspectos de segurança no acesso e circulação da informação clínica, implementa a identificação dos participantes e a segurança das operações.

4.2.3. Prescrição Electrónica de Medicamentos Centralizada

O projecto de "Receita Médica Electrónica", piloto já em funcionamento, é um exemplo da aplicação do "Cartão do Cidadão" [114] na saúde, e é um meio para melhorar, o desempenho e os benefícios de todos os actores que intervêm no processo.

Neste modelo, a receita não circula pela mão do utente. A receita é enviada para uma base de dados central de prescrições localizada no IGIF, sendo posteriormente acedida pelas farmácias (ver Figura 12 – Diagrama do Processo Prescrição Electrónica).

O processo inicia-se com a prescrição de medicamentos efectuada pelo médico ao paciente, passa pela dispensa do medicamento na farmácia e termina com a conferência de facturas dos medicamentos e respectivo pagamento da comparticipação do Estado.

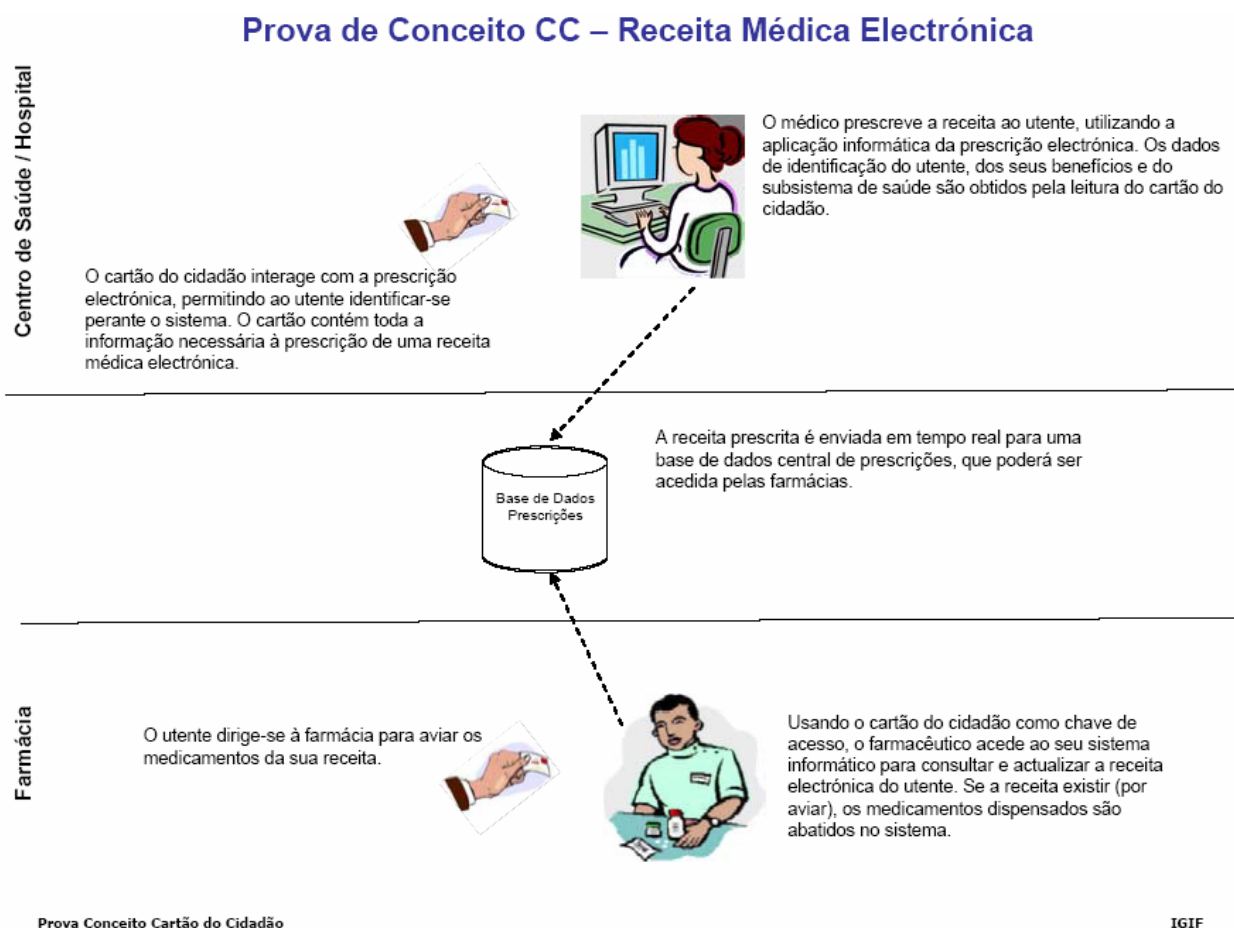



Figura 12 – Diagrama do Processo Prescrição Electrónica
(Fonte: Relatório Final Prova do Conceito)

Este sistema permitirá essencialmente atingir os seguintes objectivos: potenciar a racionalização durante o acto de prescrição (disponibilizar ao médico informação sobre os medicamentos disponíveis no mercado, acesso a informação complementar sobre o paciente, prescrições anteriores, medicação prolongada, etc.); prevenir erros e melhorar o combate à fraude, pois a receita electrónica é gerada, armazenada e manipulada, sempre no mesmo local físico (base de dados central); apenas o médico que prescreve e o farmacêutico que dispensa os medicamentos, podem visualizar e interagir com a receita electrónica.

4.2.4. O ALERT®

Para além do sistema anteriormente descrito começa a ser significativo e com tendência a aumentar a instalação e implementação de uma inovadora aplicação informática, o ALERT® [67] [68]. Esta aplicação é uma solução de natureza clínica desenvolvida em Portugal constituída por diferentes módulos (por exemplo: consulta, internamento, urgência) que permite uma maior eficácia na prestação de cuidados de saúde, nomeadamente em centros de saúde e hospitais, na medida em que possibilita o registo, a interligação de instituições, a reutilização e a análise de toda a informação relacionada com um episódio clínico do paciente. Esta solução, disponível em português, contempla todos os intervenientes profissionais na prestação de cuidados: médicos, enfermeiros, auxiliares de acção médica, técnicos de imagem e laboratório, assistentes sociais, gestores e administrativos e utentes. Assenta na utilização de monitores sensíveis ao tacto "*touch-screen monitors*", na identificação dos profissionais de saúde por impressão digital e dos utentes por pulseiras.

Ao nível técnico e funcional esta solução apresenta ainda características particulares e diferenciadoras, nomeadamente:

O ALERT® está munido de noções de *workflow*, contém um *datawarehouse*, inclui um processo clínico electrónico e está dotado da capacidade de interacção com outras aplicações através de interfaces HL7, para além de estar em conformidade com outras normas internacionais tais como: SNOMED; CIPE (ICNP); ICD9; DICOM.

A gestão de utilizadores é efectuada de forma centralizada e cada tipo de utilizador (médico, enfermeiro, administrativo, etc.) possui o seu próprio perfil, garantindo assim que a cada utilizador só é dada permissão de acesso à informação necessária para o desempenho da sua actividade, adaptando-se ainda o interface a cada um dos perfis em causa. O acesso à aplicação é efectuado por reconhecimento biométrico podendo ainda ser utilizados outros sistemas de acesso.

A gestão de utentes é efectuada centralmente, não há desta forma lugar à duplicação de informação, o que diminui o risco inerente à utilização de processos de sincronização. Os diferentes sistemas utilizarão em tempo real a informação disponibilizada por este sistema centralizado,

mantendo apenas referências aos códigos identificadores dos utentes que serão únicos em todo o Sistema de Informação.

A possibilidade de existência de uma fotografia do utente permite uma melhor identificação num ambiente crítico de urgência, uma abordagem mais pessoal ao utente para confirmação da sua identidade e uma reconstrução mental da história de um determinado episódio de urgência, assim como a associação entre uma história clínica e um determinado utente, reduzindo o período de atendimento e tornando mais fácil a prestação de cuidados de saúde de qualidade.

Os dados de referência, como por exemplo as listagens de unidades de saúde, profissionais, serviços ou codificadores, serão mantidos igualmente de forma central evitando-se a gestão de dados que são comuns por parte de outras aplicações e o recurso a mapeamentos para a troca de informação entre os mesmo.

As ferramentas para estatística, apoio à gestão e decisão, planeamento e investigação, estão todas reunidas sob um armazém de dados *"Data Warehouse"* centralizado que reunirá os dados de todos os subprodutos que compõem a solução.

Para além disto, importa realçar o facto de que a comunicação de dados através da rede é efectuada de forma cifrada.

A utilização de normas de comunicação como o HL7, DICOM ou XML, permite uma elevada interoperabilidade entre diferentes aplicações que tenham necessidade de interacção com o ALERT.

Por outro lado, ao nível da ergonomia da interface, a solução foi desenvolvida para digitação directa no ecrã (*touch screen*). As teclas de funcionamento básico têm uma representação pictográfica de modo a serem intuitivas e mnemónicas e, ao nível gráfico, o produto ALERT® tem em consideração questões relacionadas com a natureza e complexidade dos diversos ambientes de prestação de cuidados de saúde, nomeadamente através:

- da utilização de cores neutras em todo o ambiente, com excepção da cor vermelha característica da indicação de um sinal de alerta;
- do recurso a gradações da tonalidade principal nos botões de operação, traduzindo o seu estado de disponibilidade na aplicação;
- da composição geométrica dos quadros e distribuição da informação de acordo com o sentido tradicional de leitura no ocidente, em "Z", da esquerda para a direita, de cima para baixo;
- do posicionamento dos botões mais importantes nas zonas mais nobres do ecrã;
- do recurso a símbolos e pictografia universalmente reconhecível como sintaxe primária da aplicação;

– da adequação das dimensões dos elementos pictográficos à antropometria dos utilizadores, tendo em conta as dimensões do dedo indicador e das cores dos tipos gráficos, tendo em conta a distância do plano do monitor no campo visual dos utilizadores.

Toda a informação de natureza pessoal pode ser eliminada e ou alterada, sempre que se justificar, e após manifestação directa do utente. No entanto, ao nível da informação clínica, a aplicação não permite que este tipo de dados seja eliminado e ou alterado, embora se possam efectuar novos registos para correcção de anteriores, os quais permanecem guardados com um estado diferente.

O sistema permite ainda a gestão central ou local de conteúdos, permitindo que sejam adoptadas *Guidelines* ou Normas de Orientação Clínica, bem como a respectiva personalização através da criação de textos mais frequentes e "favoritos" com base numa funcionalidade designada por "My Alert".

Em conclusão, esta solução global de informatização pode criar um ambiente clínico "sem papel".

4.3. A Mobilidade na Saúde

4.3.1. Introdução

O surgimento de tecnologias de redes de comunicação móveis e sem fios (GPRS[62], UMTS[63] e Wi-Fi) em conjunto com equipamento portátil (Portáteis, Pocket PC, Tablet PC, Telemóvel, etc.), vem ao encontro das crescentes exigências do eSaúde, onde informações "agora" e "em qualquer lugar" são requisitos fundamentais e abrem conjunto de potencialidades de utilização. As redes de comunicações utilizadas, para além dos tradicionais serviços de voz, agregam novos recursos de comunicação móvel de dados. A telemedicina [100] é uma área por excelência e onde o contributo destas tecnologias é indiscutível nomeadamente em cenários de emergência médica e telemonitorização.

[62] GPRS – General Packet Radio Service.

[63] UMTS – Universal Mobile Telecommunications System.

4.3.2. Profissionais

Na Figura 13 apresentam-se algumas imagens dos terminais móveis utilizados pelos profissionais de saúde para aceder à informação clínica.

A mobilidade implica diferentes tipos de redes sem fios e dispositivos móveis no acesso à informação clínica, que acarretam novos problemas de segurança que acrescem os tradicionais problemas ligados às redes fixas.

Figura 13 – Mobilidade na Saúde

Por exemplo, os dispositivos móveis constituem uma ameaça de segurança devido à sua reduzida dimensão (equipamento fácil de perder ou roubar) e à inexistência de políticas de segurança na maioria das instituições.

Algumas medidas para proteger o acesso à transmissão e armazenamento dos dados usando equipamento móvel podem ser enumeradas (a grande maioria já foi referida em capítulos anteriores): tratar dispositivos não registados como intrusos; reforçar a utilização nos dispositivos pessoais de ferramentas de segurança; activar senhas de acesso (e considerar a activação de autenticação biométrica); utilizar mecanismos de autenticação para aceder ao servidor de informação; configurar o dispositivo para destruir informação crítica caso sejam tentados acessos não autorizados; cifrar dados armazenados; identificar bem os dispositivos na rede; cifrar dados em trânsito ponto-a-ponto (por exemplo, canal seguro SSL); monitorizar e fazer auditorias ao sistema.

No geral, nota-se que existe preocupações, mas poucos avanços em matéria de segurança no que se relaciona com estas novas tendências. Normalmente apenas são implementados os mecanismos disponibilizados nativamente pelo equipamento (ou na plataforma base), e nem sempre da melhor forma. Um factor relevante sobre a segurança da tecnologia sem fios é a escolha de equipamentos de qualidade e instalação de infra-estrutura de segurança integrada bem planeada.

Em Portugal, existem alguns exemplos de sucesso de soluções que fornecem mobilidade aos profissionais de saúde. Como referido no Capitulo 3, algumas instituições utilizam equipamento móvel no acesso ao SAPE pelos profissionais de enfermagem, cujo principal objectivo é a realização do "Plano de Trabalho" à cabeceira do paciente. Na realização do trabalho poderão ser utilizados PDAs. No acesso ao SAM também pode ser usado equipamento móvel (Tablet PC ou Portátil), o que, no entanto, ainda não está generalizado.

Outro exemplo de um projecto inovador e ainda em desenvolvimento é o projecto SAMURAI (Serviços e Aplicações Multimédia em Ambiente Hospitalar, Universitário e Urbano) [79] resultante de uma parceira entre a Universidade da Beira Interior (UBI), o Centro Hospitalar da Cova da Beira, EPE (CHCB) e a Portugal Telecom Inovação, SA (PTIN). O principal objectivo é criar e desenvolver aplicações multimédia móveis e sem fios, adequada à realização de tele-trabalho, *e*Learning e telemedicina em ambiente hospitalar, universitário e urbano. Além disso, promove a investigação em caracterização de aplicações multimédia móveis e sem fios de terceira geração (3G) e UMTS, e utilização de conceitos de design ergonómico no seu desenvolvimento.

De forma a disponibilizar estas novas tecnologias no ensino e teletrabalho hospitalar na UBI e no CHCB [81], foi concebido e implementado uma rede local sem fios *Wi-Fi* no Hospital Pêro da Covilhã (HPC), constituída por algumas dezenas de APs, de forma a fazer a cobertura das áreas mais importantes do hospital.

No âmbito deste projecto, um dos objectivos é a expansão progressiva deste modelo de infra-estrutura de rede sem fios e aplicações *web* aos hospitais da Guarda (Hospital Sousa Martins), HPC e de Castelo Branco (Hospital Amato Lusitano), naquele que será o primeiro passo para a criação de uma aldeia global na saúde da Beira Interior.

Em simultâneo com a implementação da infra-estrutura de rede sem fios, foram realizados estudos no sentido de instalar, desenvolver ou adaptar aplicações à tecnologia *"web based"* e ao tipo de equipamento a utilizar (PDAs, Tablet PCs, etc.).

Na Figura 14 apresentam-se algumas imagens dos terminais móveis utilizados para aceder a aplicações do HPC.

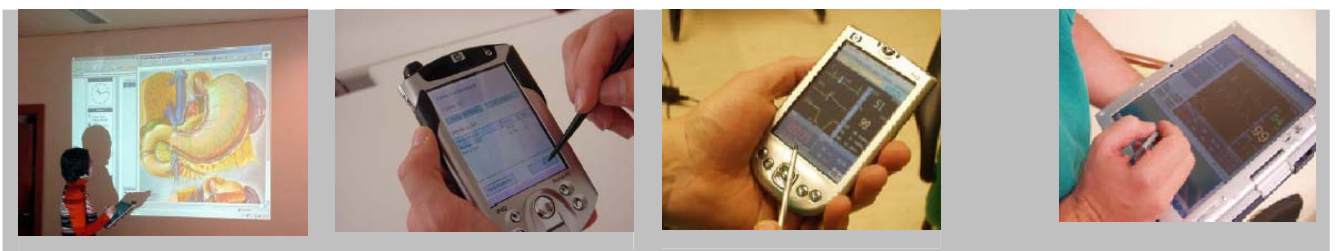



Figura 14 – Exemplos de aplicação de terminais móveis no acesso a aplicações clínicas

Para garantir a interoperabilidade e compatibilidade entre equipamentos e mecanismos de segurança, destaca-se a conformidade do equipamento com a norma IEEE 802.1g e certificação *Wi-Fi*. A configuração da rede prevê: a instalação de um servidor RADIUS (Remote Authentication Dial In User Service) para autenticação dos utilizadores na rede sem fios; isolamento de tráfego

"sem fios" na mesma VLAN; um servidor DHCP[64], de onde todas as estações clientes recebem todos as configurações necessárias para um correcto funcionamento.

Ainda em fase de projecto [80], e para implementar a necessária interoperabilidade entre a rede sem fios de área metropolitana de banda larga (Wireless Metropolitan Área Network - WMAN) – (Worldwide Interoperability for Microwave Access - WiMAX), para interligar ponto-a-ponto os hospitais, e uma rede ponto-multiponto para ligar a UBI a toda a área urbana da cidade da Covilhã, será necessário a instalação de um uma antena de WiMAX na serra da Gardunha. O planeamento desta infra-estrutura, as ligações radioeléctricas WiMAX, estão conforme as normas IEEE 802.16 (Especificação para WMANs nas frequências entre 2 e 11 GHz) e IEEE 802.21 (Especificações para interoperabilidade de redes heterogéneas incluído as duas 802 ou não).

4.3.3. Pacientes

A telemonitorização (ou TeleHomeCare) poderá trazer ganhos indescritíveis para a qualidade de vida do utente, reduzindo significativamente as necessárias idas ao hospital (clínicas, centro de saúde, ou outras entidades de saúde), para monitorização da sua doença. A telemonitorização consiste no envio de sinais biológicos, imagens médicas, dados laboratoriais, desde o local do paciente a um centro especializado de monitorização, interpretação e análise.

Os aspectos a monitorizar são diversos: dispositivos biomédicos de rastreio portáteis para monitorização de sinais vitais (peso, frequência cardíaca, tensão arterial, etc.); sistemas domésticos de comunicação interactiva que ligam o utente com o prestador de cuidados de saúde, a quem é proporcionado formação e orientação; sensores integrados em vestuário (ver Figura 16); processamento automático e local (no dispositivo do paciente); algoritmos de interpretação inteligentes.

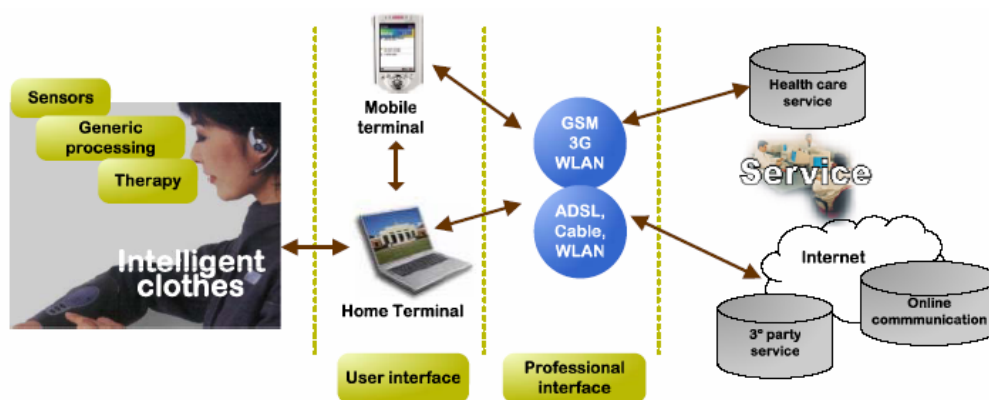
---

[64] DHCP – Domain Host Control Protocol, é um protocolo que permite a configuração dinâmica de clientes de rede atribuídos endereços IP e outros parâmetros. Especificações RFC 2131 e 3315.

Figura 15 – Tendências da Telemonitorização

(Fonte: Apresentação "Vencer as doenças cardiovasculares: a contribuição de engenharia" [105])

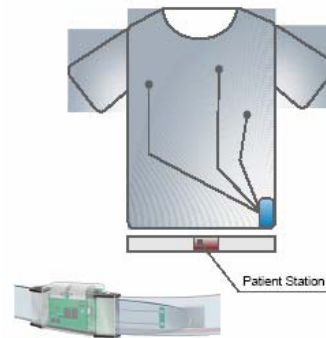



Figura 16 – Sensores integrados no vestuário

(Fonte: Apresentação "Vencer as doenças cardiovasculares: a contribuição de engenharia" [106])

Por exemplo, em Portugal, o seu uso no apoio individualizado à rotina do auto tratamento de pacientes asmáticos crónicos seria um projecto muito interessante, que permitiria manter os pacientes saudáveis e evitar visitas desnecessárias aos hospitais. A disponibilização de equipamentos portáteis (espirómetro digital) por parte do SNS, sem encargos para o utente, podia ser feita tal como já acontece para outro tipo de equipamentos (por exemplo nubelizador, etc.). Uma das tendências em TeleHomeCare será a sua aplicação na especialidade de TeleGeriatria no apoio ao paciente idoso.

Em Portugal, o projecto MyHeart [105] [106] [107], em curso (termo em 2007) que envolve vários parceiros (indústria, universidades e hospitais), tem por missão combater as doenças cardiovasculares através do diagnóstico precoce, e pretende o desenvolvimento de algoritmos de diagnóstico que se adaptem às especificidades dos doentes e o desenvolvimento de sistemas minimamente intrusivos pela integração de sensores em vestuário. Tem já duas aplicações distintas: gestão preventiva de próteses valvulares (Figura 17) e avaliação de arritmias ventriculares (Figura 18).

Figura 17 – Gestão preventiva de próteses valvulares.

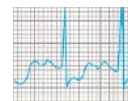



Figura 18 – Avaliação de arritmias ventriculares

Outro projecto, MobiHealth [108], que se tem revelado de grande sucesso na área da monitorização do paciente, é um projecto "Wireless Body Area Network" para cuidados de saúde, e visa o desenvolvimento e experimentação de novos serviços e aplicações na área da saúde móvel, promovendo o uso e a disponibilização das tecnologias GPRS e UMTS (ver Figura 19). O seu

principal objectivo é monitorizar os sinais vitais do paciente remotamente recorrendo à infra-estrutura de rede móvel pública, a dispositivos portáteis (PDAs, telemóveis, etc.) e a sensores médicos.

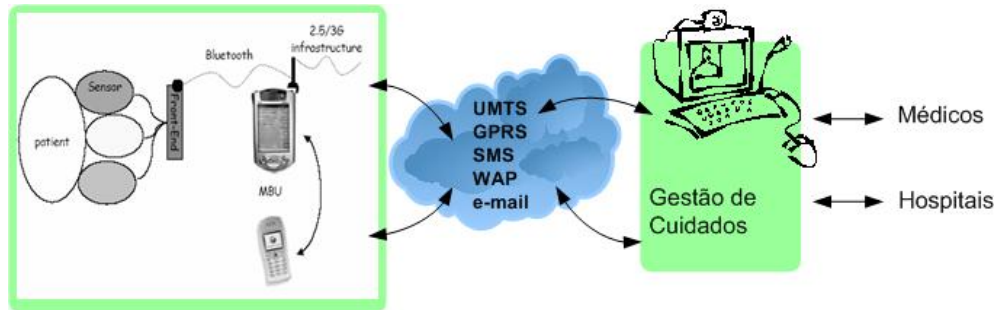



Figura 19 – Sistema MobiHealth

4.4. O VOIP na Saúde

Um dos serviços avançados de rede que a RIS promove junto das instituições é a integração de voz e dados na mesma infra-estrutura de rede. Trata-se de dos grandes objectivos a atingir com a globalização da rede.

Inovações recentes tornaram possíveis chamadas telefónicas pela Internet ou a intranet da saúde, conhecidas também como VoIP[65]. Trata-se de uma tecnologia que vem sendo cada vez mais adoptada pelas empresas em todo o mundo devido à economia alcançada com a sua implantação, operação e manutenção. Em média, estima-se uma economia de cerca de 80%, quando comparada com a solução de uma central telefónica tradicional.

A telefonia na Internet refere-se a serviços de comunicação (voz, fax, aplicações de mensagens de voz, etc.) que são transportadas pela Internet ou RIS em vez da rede telefónica comutada convencional.

Os problemas de segurança relacionados com o VoIP na RIS, basicamente são os memos que ocorrem noutro tipo de redes TCP/IP. As redes VoIP são um alvo importante, pois, como exemplo, poderiam ser capturadas informações clínicas, administrativas ou financeiras importantes para a instituição, cuja utilização poderia significar perdas irreparáveis. As principais ameaças ao VoIP são mais ou menos idênticas às que já foram apontadas em comunicações e Internet, sendo de realçar o caso da negação de serviços que iria paralisar os serviços disponibilizados.

[65] VoIP - Voice Over Internet Protocol.

Algumas soluções para melhorar a segurança no VoIP seriam: segmentar o tráfego; usar *firewalls* especializadas em filtrar toda informação que seja ou não endereçada a rede de voz; implementar um sistema IDS; usar preferencialmente telefones IP e não aplicações IP Phone (programas de telefonia instalados nos computadores), pois computadores com sistemas operativos são mais susceptíveis a ataques; usar endereços privados e inválidos para dificultar ou proibir o acesso externo do ambiente de trabalho; configurar telefones IP com endereços IPs estáticos; utilizar DHCP separados para dados e voz; implementar mecanismos de autenticação dos utilizadores em telefones IP; etc.

Onde há convergência das redes, também há convergência das ameaças, portanto a tecnologia de voz sobre IP ainda herda as vulnerabilidades das redes TCP/IP, e ainda hoje não existem soluções de segurança perfeitas ou completas. Então, um factor relevante sobre a segurança da tecnologia de voz sobre IP é a escolha dos equipamentos de qualidade e infra-estrutura bem planeada.

4.5. Conclusão

Existem inúmeras tecnologias em desenvolvimento e que irão certamente ganhar destaque a curto prazo: novas especialidades na telemedicina, utilização de cartões com chips identificativos, etc.

A evolução contínua sustentada e integrada das plataformas de trabalho cooperativo existentes no mercado português permite atingir um cada vez maior número de especialidades clínicas.

Algumas das tecnologias que prometem ajudar neste desafio são: uso de ambientes gráficos atraentes e amigáveis; incorporar nos sistemas reconhecimento de voz; tecnologias *touch-screen* (por exemplo, ALERT®); sistemas de processamento de linguagem natural (por exemplo, a partir de texto livre introduzido o sistema retira informação codificada), introdução de informação estruturada de forma dinâmica e adaptada a cada utilizador; monitores de alta definição (por exemplo, para visualização de imagem médica); redes informáticas de grande velocidade; utilização de equipamento portátil para introdução e visualização dos dados clínicos (por exemplo: PDAs, Tablet PC, nova geração PDA/mini PC, telemóvel); incorporação de sistemas de monitorização nos registos clínicos (por exemplo: monitorização contínua em unidades de cuidados intensivos); sistemas de apoio à decisão clínica na tomada de decisões de diagnóstico e de terapêutica nos cuidados a pacientes. Este sistemas consistem numa base de conhecimento e num mecanismo de inferência e que utilizando dados clínicos recolhidos geram recomendações específicas para cada caso específico.

Algumas tecnologias que poderão emergir no futuro são a "Realidade Virtual em Medicina", que passa pela criação de modelos médicos virtuais de forma gráfica onde os médicos podem praticar situações reais; e a "Robótica Médica" que passa pelo uso de robôs para realizar cirurgias à distância. Através da Internet, começa a esboçar-se a formação de uma nova estrutura de interacção entre pessoas e máquinas, o ciberespaço médico. Com o uso dos recursos da Internet (o correio electrónico, as listas de discussão, a *web*, etc.), uma "Comunidade Médica Virtual" ou "Hospital Virtual" não é impossível. Outra tecnologia que já se apresenta de grande valor para o progresso do conhecimento médico é a gigantesca base de dados MEDLINE, acessível pelo sistema PubMed, para acesso à informação científica para fins educacionais e assistenciais.

A introdução de novas tecnologias coloca sempre novos desafios, e um desses novos desafios é a segurança. Com o surgir de novos conceitos, processos, tecnologias e serviços, as questões relacionadas com a segurança no acesso, circulação e armazenamento da informação clínica devem ser repensadas e analisadas cuidadosamente. Por exemplo, as soluções sem fios são uma das componentes da tecnologia da informação a ter em conta no desenho de novas arquitecturas que colocam novos desafios nas questões de segurança. Estas soluções, através do uso de dispositivos móveis, permitem disponibilizar a capacidade de computação no local e no momento em que é requerido pelo profissional de saúde ou o paciente.

Apesar das inúmeras vantagens na utilização de sistemas VoIP na Saúde, e existirem condições para a sua prática, não são conhecidas implementações efectivas em larga escala.

Sendo algumas das tecnologias relativamente recentes, ainda não foram desenvolvidos os mecanismos mais adequados à sua utilização de uma forma segura. Os mecanismos incorporados nas próprias soluções têm-se mostrado inadequados ou, mesmo quando existem, não são implementados da forma mais correcta.

Muitas das questões de segurança que se colocam poderão ser minimizadas com o uso do Cartão do Cidadão na sua interacção com o SNS. No caso das novas tendências no domínio da telemedicina, a segurança consegue-se usando mecanismos de autenticação forte nos casos em que é aplicável. Nos casos em que não é aplicável, existem outros mecanismos capazes de oferecer segurança nas comunicações (VPNs, SSL, etc.).

5 PROPOSTAS PARA A MELHORIA DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO CLÍNICA

Neste capítulo propõe-se um conjunto de medidas globais para a melhoria da segurança dos sistemas de informação clínica das unidades de saúde tuteladas pelo MS (hospitais, centros de saúde, IGIF, etc.).

Com a tendência da centralização dos sistemas de informação clínica, a criação de bases de dados remotas (por exemplo: SIGIC, referido no Capítulo3), a utilização da telemedicina, a crescente partilha de informação clínica interinstitucional (via correio electrónico, *web*, etc.), a centralização dos registos clínicos do paciente, a centralização de prescrição electrónica de medicamentos, a circulação da informação clínica dentro da RIS e através das suas fronteiras coma Internet tem aumentado imenso.

Surge assim a necessidade de utilização de políticas e mecanismos de segurança que garantam a confidencialidade dos dados, sua integridade, o "não repúdio" de acções, e que tenham uma abrangência global, não podendo ser confinadas a unidades de saúde isoladas.

Assim as propostas de melhoria de segurança informática aqui sugeridas vão no sentido de se:

- Implementar um "Plano de Segurança Global", a aplicar a todas as unidades de saúde que integram a RIS e a outras entidades privadas com a qual exista articulação (hospitais privados, clínicas privadas, laboratórios, farmácias, etc.).

- Implementar uma infra-estrutura de chaves públicas, em que o Ministério da Saúde ficará dotado de uma autoridade de certificação própria para emissão de certificados digitais.

Na base destas propostas estão os seguintes pressupostos:

- O IGIF é a entidade responsável pela gestão e intervenção técnica na RIS e de grande parte dos sistemas de informação clínica instalados nas unidades de saúde, tendo um papel normalizador e global;
- O IGIF será a entidade responsável pela gestão global da "Política de Segurança" do Ministério da Saúde;
- O IGIF será a entidade responsável pelo topo da infra-estrutura de chaves públicas do Ministério da Saúde;

– A centralização da informação clínica (em "data-center") será uma realidade a curto prazo.

Assume-se ainda que cada instituição ou organização possui um ambiente distinto, os seus próprios requisitos de segurança e características peculiares, devendo portanto desenvolver ou moldar uma política de segurança adequada que estenda e complemente a política de segurança global.

A proposta de implementação de uma "Politica de Segurança Informática para o Ministério da Saúde" a seguir apresentada foi elaborada tendo por base a norma ISO 27779 – *Security Management in Health Using ISO/IEC 17799*. A proposta cobre alguns pontos relevantes da norma, sendo de evidenciar os requisitos de segurança no que se relaciona com a política de gestão de senhas, os direitos e responsabilidades dos utilizadores e dos departamentos de TICs[66] na saúde, e as acções previstas em caso de violação das políticas.

Também a proposta de implementação de infra-estrutura de chave-pública para o Ministério da Saúde baseia-se na norma ISO 17090 – *Public Key Infrastructure, Health Informatics*. A proposta assenta numa estrutura hierárquica em que a entidade de topo é a recém criada ECEE[67], a entidade responsável pela emissão dos certificados o IGIF e as instituições de forma individual ou agrupada são responsáveis pela gestão de parte do ciclo de certificação interno às suas instituições. Na interacção dos profissionais de saúde com o sistema, recomenda-se o uso de um cartão profissional único para identificação, autenticação e controlo de acesso físico.

Todas as propostas apresentadas têm por finalidade estabelecer orientações genéricas que deverão ser adoptadas pelas instituições que integram o MS e deverão ser embebidas noutros processos das organizações.

---

[66] TICs – Tecnologias de Informação e Comunicações.

[67] ECEE – Entidade Certificadora Electrónica do Estado. Foi criada em 2005 através da Resolução do Conselho de Ministros n.º 171/2005, de 03/11 – Série I-B-nº211 [55].

5.1. Proposta de Política de Segurança Informática para o Ministério da Saúde

Uma boa política de segurança informática é uma directiva importante no sentido de proteger as instituições contra ameaças à segurança da informação que lhes pertence ou que está sob a sua responsabilidade (por exemplo, informação clínica do paciente). Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais das suas propriedades fundamentais, a confidencialidade, integridade e disponibilidade.

Alguns factores importantes para o sucesso desta política de segurança são o envolvimento e apoio por parte dos conselhos de administração das instituições, para além de que todos os utilizadores devam tomar conhecimento e manifestar a sua concordância em submeter-se a ela antes de obter acesso aos recursos informáticos.

O objectivo desta política de segurança não é definir procedimentos específicos de manipulação e protecção da informação clínica, mas sim atribuir direitos e responsabilidades aos profissionais de saúde que lidam com essa informação. Desta forma, eles sabem quais são as suas atribuições em relação à segurança dos recursos informáticos com os quais trabalham. Além disso, a política de segurança também estipula as penalizações a que poderão estar sujeitos caso não cumpram com as suas atribuições.

Estas orientações servirão de base a normas e procedimentos de segurança a serem elaborados e implementados por cada instituição, considerando as suas particularidades.

Os objectivos da política de segurança informática são: definir o âmbito de segurança informática das instituições; fornecer orientações de segurança às instituições, para reduzir riscos e garantir a integridade, sigilo e disponibilidade da informação clínica, dos sistemas e recursos; permitir a adopção de soluções de segurança integradas; servir de base para auditorias e avaliação de responsabilidades.

Esta política de segurança abrange os seguintes aspectos [126]: requisitos de segurança gerais, humana, física e lógica.

5.1.1. Requisitos de segurança gerais

A política de segurança informática para o MS aplica-se a todos os recursos humanos e tecnológicos pertencentes às instituições que o compõem. A abrangência dos recursos citados refere-se tanto àqueles ligados às instituições em carácter permanente como aos de carácter temporário.

A política de segurança deve ser comunicada a todos os profissionais envolvidos (por exemplo: administrativos, enfermagem e médicos) e amplamente divulgada através da instituição, garantindo que todos a conheçam e cumpram.

Um programa de sensibilização sobre segurança da informação em geral deverá ser elaborado para assegurar que todos os profissionais sejam informados sobre os potenciais riscos de segurança a que estão sujeitos os sistemas e actividade da instituição. Especificamente, os utilizadores devem estar informados sobre ataques típicos de engenharia social e de como se proteger deles.

Os procedimentos deverão ser documentados e implementados para garantir que quando os profissionais de saúde contratados ou prestadores de serviços são transferidos, dispensados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.

Deve existir um mecanismo de armazenamento centralizado para manutenção de rastos, registos de *logs* e outras notificações de incidentes. Estes mecanismos deverão ser incluídos nas medidas a serem tomadas pelo grupo responsável pela segurança e integrados nas medidas de defesa activa e correctiva da instituição.

O processo de gestão de riscos deve ser revisto periodicamente pela instituição, para prevenir riscos (inclusive aqueles com origem nas novas tecnologias), com o objectivo de elaborar planos de acção apropriados para protecção aos componentes ameaçados. Para tal ser possível, todos os activos das instituições devem estar inventariados, classificados e os registos mantidos permanentemente actualizados.

Um plano de contingência deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos (por exemplo, sistemas de suporte de vida ou emergência). Devem também ser definidos planos de gestão de incidentes e de acções de resposta a incidentes.

Os certificados das instituições deverão ser imediatamente revogados pelo IGIF se um evento provocar a perda ou comprometimento de sua chave privada ou do seu meio de armazenamento.

5.1.2. Requisitos de segurança dos utilizadores

Nesta secção é sugerido um conjunto de medidas e procedimentos de segurança, a serem observados pelos profissionais de saúde ou outros prestadores de serviço, para a protecção dos activos das instituições. Estas medidas visam: reduzir os riscos de erros humanos, furto, roubo, fraude ou uso não apropriado dos activos da instituição; prevenir e neutralizar as acções sobre as pessoas que possam comprometer a segurança da instituição; orientar e dotar de competências todo os profissionais envolvidos na realização de trabalhos directamente relacionados com os registos clínicos do paciente, assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adopção de medidas de protecção compatíveis com a natureza da função que desempenham.

a) Orientações no Processo de Gestão dos Profissionais de Saúde

Devem ser adoptados critérios rígidos para o processo de selecção de candidatos, com o propósito de seleccionar pessoas de idoneidade reconhecida e sem antecedentes que possam comprometer a segurança ou credibilidade da instituição e os registos pessoais do paciente. O profissional de saúde ou prestador de serviços deverá assinar um termo de compromisso, assumindo o dever de manter sigilo, mesmo quando desligado das suas funções, sobre todos os activos de informações e de processos da instituição, em particular, sobre a informação relacionada com o paciente.

De acordo com a actividade a desenvolver devem relacionar-se as tarefas inerentes a cada função, a fim de se determinar o perfil necessário do profissional. Para além disto, deve-se acompanhar o desempenho e avaliar periodicamente os profissionais com o propósito de detectar a necessidade de formação ou actualização técnica e de segurança. Eles devem ser identificados por meio de credenciais, permitindo o acesso a informações sensíveis, de acordo com a classificação do grau de sigilo da informação e o grau de sigilo compatível com o cargo e/ou a função desempenhada. Também deverá estar definido o processo de desvinculação de um funcionário ou prestador de serviço da instituição. O acesso de ex-colaboradores às instalações deve ser vedado e revogadas as credenciais e todos os mecanismos de acesso (físicos ou lógicos, por exemplo: crachá) por eles antes utilizados.

Deve-se definir a forma de apresentar aos colaboradores e prestadores de serviço a política de segurança da informação e as normas e procedimentos relativos ao tratamento da informação e/ou dados sigilosos, com o propósito de desenvolver e manter uma efectiva sensibilização de segurança, assim como instruir o seu fiel cumprimento.

b) Responsabilidades dos funcionários

Em geral, todos os profissionais têm o dever de preservar a integridade e guardar sigilo da informação de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informação clínica, sob pena de incorrer nas sanções disciplinares e legais aplicáveis.

Devem utilizar os sistemas de informações das instituições e os recursos a elas afectos somente para os fins previstos; não devem partilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso, em particular, informação clínica dos pacientes; devem manter o carácter sigiloso da senha de acesso aos recursos e sistemas, podendo vir a ser sujeitos a responder por todo e qualquer acesso indevido aos recursos da instituição efectuados através do seu código de identificação.

Em caso de tomarem conhecimento de qualquer irregularidade ou desvio que possa levar a quebras de segurança, devem comunica-lo ao seu superior imediato.

– *Chefias*

É dever dos responsáveis pelos serviços garantir que o pessoal sob sua supervisão compreende e desempenha a obrigação de proteger a informação da instituição.

Devem comunicar formalmente ao serviço que atribui privilégios aos utilizadores, quais os colaboradores sob sua supervisão, que podem ter acesso à informação e a que tipo e comunicar os nomes dos colaboradores demitidos ou transferidos, para exclusão no cadastro dos utilizadores que ficaram assim, impedidos de aceder aos activos de informação e de processamento relacionados com a sua área de actuação.

– *Gestor de Segurança*

Cabe ao gestor de segurança a responsabilidade de definir e aplicar, para cada utilizador, as restrições de acesso à rede (horário autorizado, tipo de utilização, etc.) e controlar os privilégios de utilizadores remotos e externos (por exemplo, manutenção remota por empresas externas à RIS), devendo detectar, identificar, registar e comunicar ao IGIF as violações ou tentativas de acesso externo não autorizadas (i.e., tentativas de acesso provenientes da RIS).

Deve manter registos das actividades dos utilizadores por um período alargado (por exemplo, 5 anos) que devem conter: hora e data das actividades, a identificação do utilizador, comandos e argumentos executados, identificação do posto de trabalho (local ou remoto) que efectuou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc.).

Deve fornecer senhas de contas privilegiadas somente aos colaboradores que necessitem efectivamente dos privilégios, mantendo registos e controlar essas permissões.

Deve também limitar o prazo de validade das contas dos contratados ou prestadores de serviço ao período da contratação.

Para alem destas responsabilidades, devem ainda decidir as medidas a serem tomadas no caso de violação das regras estabelecidas; estabelecer as regras de protecção dos activos; efectuar a revisão anual das regras de protecção estabelecidas; elaborar e manter actualizado o Plano de Contingência (ver à frente); e executar as regras de protecção estabelecidas pela Política de Segurança.

c) <u>Sanções</u>

As previstas pela legislação vigente, e outras aprovadas pela direcção ou administração da instituição.

5.1.3. Requisitos de segurança do ambiente físico

As responsabilidades pela segurança física dos sistemas de informação para a saúde deverão ser definidos e atribuídos a colaboradores claramente identificados na instituição. Os sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso ao sistema de informação.

Os sistemas de informação clínica deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência electromagnética, muitas vezes associadas com o equipamento médico.

Os recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controlo de acesso; fisicamente deverão estar protegidos de acesso não autorizado, danos, ou interferência. A entrada e saída, nestas áreas ou partes, deverão ser automaticamente registadas com data e hora, o que será depois verificado periodicamente pelo responsável pela gestão de segurança da informação. Para além disto, o acesso aos componentes da infra-estrutura, actividade fundamental ao funcionamento dos sistemas das instituições, como quadros de energia, comunicações e cablagem, deverá ser restrito a pessoal autorizado. Devem ser instalados e testados regularmente sistemas de detecção de intrusos de forma a cobrir os ambientes (por exemplo, portas e janelas acessíveis) onde ocorrem processos de saúde críticos.

5.1.4. Requisitos de segurança do ambiente lógico

A informação de saúde deve ser protegida de acordo com o seu valor, fragilidade e criticidade. Para tal, deve ser elaborado um sistema de classificação da informação.

Os dados de saúde, as informações e os sistemas de informação da instituição e sob sua guarda, devem ser protegidos contra ameaças e acções não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

As violações de segurança devem ser registadas e esses registos devem ser analisados periodicamente com o propósito correctivo, legal e de auditoria. Os registos de saúde devem ser protegidos e armazenados de acordo com a sua classificação.

Os sistemas e recursos que suportam funções críticas (por exemplo: sistemas de suporte de vida e monitorização em cuidados intensivos) devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão da informação, deve estar registado e mantido actualizado em intervalos de tempo definidos pela instituição.

a) Sistemas

As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis na instituição. A documentação dos sistemas deve ser mantida actualizada. As cópias de segurança devem ser testadas e mantidas em boas condições.

Os sistemas devem possuir controlo de acesso de modo a assegurar o uso apenas a utilizadores ou processos autorizados. Os arquivos de registos devem ser criteriosamente definidos para permitir a recuperação de dados nas situações de falhas, a auditoria nas situações de violações de segurança e a contabilização do uso de recursos. Os registos devem ser periodicamente analisados para se identificar tendências, falhas ou usos indevidos. Para além disto devem ser protegidos e armazenados de acordo com sua classificação. Devem ainda ser estabelecidas e mantidas medidas e controlos de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto à sua precisão, consistência e integridade.

Os sistemas para registos de informação clínica devem ser avaliados em relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para produção. As vulnerabilidades do ambiente instalado devem ser avaliadas periodicamente e as recomendações de segurança devem ser adoptadas.

b) Servidores

O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações devem ser revistas, confirmadas e registadas continuamente.

Os acessos lógicos devem ser registados em registos, devendo ser analisados periodicamente. O tempo de retenção dos arquivos de registos e as medidas de protecção associadas devem estar precisamente definidos.

Devem ser adoptados procedimentos sistematizados para monitorizar a segurança do ambiente em que opera o sistema de informação clínico. Os eventos devem ser armazenados em *logs* de modo que sua análise permita a rastreabilidade e auditoria a partir destes registos. Para isso as

máquinas devem estar sincronizadas para permitir a rastreabilidade dos eventos. Poderá ser adoptada protecção lógica adicional (criptografia) para evitar o acesso não autorizado a esta informação.

A versão do sistema operativo, assim como outro *software* de registo clínico instalado em servidores, devem ser mantidos actualizados, em conformidade com as recomendações dos fabricantes. Dever-se-á ainda ser utilizado somente *software* licenciado ou autorizado, nomeadamente pela CNPD.

Para evitar ameaças à integridade e sigilo da informação clínica, o acesso remoto aos servidores deve ser realizado adoptando mecanismos de segurança. Para além disto, os procedimentos de cópia de segurança e de recuperação devem estar documentados, e mantidos actualizados e regularmente testados, de modo a garantir a disponibilidade da informação clínica. Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e vermes) devem estar sistematizados.

c) *Infra-estrutura de rede da instituição*

O tráfego ou trânsito de informação clínica na rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevida. Componentes críticos da rede local (por exemplo: encaminhadores e servidor de nomes) devem ser mantidos em salas próprias e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

A configuração de todos os activos de processamento deve ser verificada aquando da instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses activos.

O uso de senhas deve estar submetido a uma política específica de gestão de utilização.

O acesso lógico aos recursos da rede local deve ser realizado por meio de um sistema de controlo de acesso. O acesso deve ser concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada utilizador.

A conexão com outras redes (por exemplo, redes sem fios) e alterações internas na sua topologia e configuração devem ser formalmente documentados e guardados, de forma a gerar um registo histórico. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos actualizados.

Devem ser definidos relatórios de segurança de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os registos devem ser analisados periodicamente e o período de análise estabelecido deve ser o menor possível.

A alimentação eléctrica para a rede local deve ser separada da rede convencional, devendo ser observadas as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas aplicáveis.

O tráfego de dados deve ser monitorizado, a fim de verificar sua normalidade, e detectar situações anómalas do ponto de vista da segurança. Informação sigilosa que possa causar prejuízo ao paciente deve estar protegida e não ser enviada para outras redes sem protecção adequada. Os registos de eventos devem ser analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

A segurança das comunicações da rede interna com as redes externas deverá ser garantida pelo uso de mecanismos que assegurem o sigilo e a integridade da informação clínica em trânsito. Para tal poderão ser utilizados mecanismos de segurança baseados em sistemas de protecção de acesso (por exemplo, *firewalls*). Na rede interna, ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança.

As conexões de rede devem ter activos sistemas com função de certificação. Se isto não for possível, deve-se utilizar outros mecanismos que executem funções semelhantes tais como o uso de *proxies*.

Deverão ser implementadas ferramentas de detecção de intrusos para monitorização das redes críticas, alertando os administradores das redes sobre as tentativas de intrusão.

d) Controlo de Acesso Lógico

Utilizadores e aplicações que necessitem ter acesso a recursos da instituição devem ser identificados e autenticados. O sistema de controlo de acesso deve manter registos que permitam a contabilização do uso, auditoria e recuperação nas situações de falha. A informação que especifica os direitos de acesso de cada utilizador ou aplicação deve ser protegida contra modificações não autorizadas. Além disto, nenhum utilizador deve ser capaz de obter os direitos de acesso de outro utilizador.

As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas).

O arquivo de senhas deve ser cifrado e ter o acesso controlado. As senhas devem ser individuais, secretas, intransmissíveis e protegidas com grau de segurança compatível com a informação associada e, o sistema de controlo de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias. As seguintes características das senhas devem estar definidas de forma adequada: conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade

máximo, forma de troca e restrições específicas. A distribuição de senhas aos utilizadores deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser alterada pelo utilizador no primeiro acesso. O sistema de controlo de acesso deve permitir ao utilizador alterar sua senha sempre que o desejar. A troca de uma senha bloqueada só deve ser executada após a identificação do utilizador. A senha digitada não deve ser exibida.

Devem ser adoptados critérios para bloquear ou desactivar utilizadores em caso de tentativas sucessivas de acesso mal sucedidas e em caso de ausência ao serviço por período pré-definido. O sistema de controlo de acesso deve solicitar nova autenticação após certo tempo de inactividade da sessão (*timeout*). O sistema de controlo de acesso deve exibir, no ecrã inicial, uma mensagem informando que o serviço só pode ser utilizado por utilizadores autorizados. No momento de conexão, o sistema deve exibir para o utilizador informações sobre o último acesso.

O registo das actividades do sistema de controlo de acesso deve ser definido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os *logs* devem ser periodicamente analisados.

e) Postos de Trabalho

Os postos de trabalho devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos. Equipamentos que executem operações sensíveis devem ter protecção adicional, considerando os aspectos lógicos (controlo de acesso e criptografia) e físicos (protecção contra furto ou roubo do equipamento ou componentes).

Devem ser adoptadas medidas de segurança lógica referentes a combate a vírus, cópia de segurança, controlo de acesso e uso de *software* não autorizado. A instituição deverá estabelecer os aspectos de controlo, distribuição e instalação de *software* utilizados.

Informações sigilosas cuja divulgação possa causar prejuízo à instituição ou paciente, só deve ser utilizadas em equipamentos da instituição onde foram geradas ou naqueles por ela autorizado, com controlos adequados.

O acesso às informações deve atender aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou colectivo).

A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios clínicos impressos devem ser protegidos contra perda, reprodução e uso não autorizado.

Os sistemas em uso devem solicitar nova autenticação após certo tempo de inactividade da sessão (*time-out*).

Procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e vermes) devem estar sistematizados e devem abranger também as estações de trabalho, e os equipamentos portáteis.

5.1.5. Auditoria

O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de utilizadores e pacientes. As auditorias têm como principal objectivo verificar o cumprimento da política de segurança e das normas e procedimentos de segurança definidos.

A auditoria deve abordar os aspectos relativos ao ambiente de operação: segurança de pessoal; segurança física; segurança lógica, segurança de telecomunicações; segurança de recursos criptográficos (por exemplo, certificados digitais); plano de contingência.

5.1.6. Gestão de Riscos

A gestão de riscos é um processo que visa a protecção dos serviços das instituições, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Devem ser identificados os seguintes pontos: o que deve ser protegido; contra quem ou contra o quê deve ser protegido (análise de riscos); e efectuada uma avaliação de riscos (análise da relação custo/benefício).

Deve ser monitorizado a eficácia do controlo adoptado para minimizar os riscos identificados e devem ser periodicamente avaliados os riscos em intervalos de tempo não superiores a 6 (seis) meses, devem também serem efectuadas.

Sistematizando, a gestão de riscos consiste nas seguintes fases principais:

Identificação dos recursos a serem protegidos – hardware, rede, software, dados, informações pessoais, documentação;

Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligência) ou de qualquer outro tipo (incêndios);

Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;

Tratamento dos riscos (medidas a serem adoptadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco.

Por seu lado os riscos a serem avaliados podem ser divididos nos seguintes segmentos:

Dados e Informação - Indisponibilidade, Interrupção (perda), interceptação, modificação, fabricação, destruição;

Pessoas - Omissão, erro, negligência, imprudência, imperícia, sabotagem, amnésia;

Rede - Acesso não autorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço;

Hardware - Indisponibilidade, interceptação (furto ou roubo), falha;

Software e sistemas - Interrupção, interceptação, modificação, desenvolvimento, falha;

Recursos criptográficos - Ciclo de vida dos Certificados Digitais;

5.1.7. Plano de Contingência

O Plano de contingência é um documento cujo objectivo é permitir manter em funcionamento os serviços e processos críticos das instituições, na eventualidade da ocorrência de desastres, atentados, e falhas diversas.

Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

Todas as instituições deverão elaborar um tal plano de contingência que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança: comprometimento da chave privada da instituição; invasão do sistema e da rede interna da instituição; incidentes de segurança física e lógica; indisponibilidade da infra-estrutura.

Todo o pessoal envolvido com o plano de contingência deve receber formação específica para poder enfrentar estes incidentes. Um plano de acção de resposta a incidentes deverá ser estabelecido pela instituição que deve prever, no mínimo, o tratamento adequado dos seguintes eventos: comprometimento de controlo de segurança em qualquer evento referenciado no Plano de Contingência; notificação à comunidade de utilizadores, se necessário; revogação dos certificados cujas chaves correspondentes tenham sido comprometidas; procedimentos para interrupção ou suspensão de serviços e investigação; análise e monitorização de rastos de auditoria; relacionamento com o público e com meios de comunicação se necessário.

5.2. Proposta de Infra-estrutura de Chaves Públicas para o Ministério da Saúde

Ao longo dos últimos anos, as infra-estruturas de chave pública (PKI[68]) têm merecido um interesse crescente pelas suas vantagens relativas à utilização de infra-estruturas de chaves secretas para dar segurança aos sistemas informáticos.

Esta proposta assenta numa estrutura hierárquica de certificação de chaves públicas em que a entidade de topo seria a recém criada ECEE, a entidade certificadora associada, para a área da Saúde, seria o IGIF e as instituições de forma individual ou agrupada seriam responsáveis pela gestão do ciclo de certificação interno às suas instituições. Sugere-se o IGIF como autoridade certificadora para a área da Saúde porque, para além de ter um papel normalizador, já é a entidade responsável pela gestão da RIS e de grande parte das aplicações instaladas nas unidades de saúde e possui os meios para actuar ao nível desta infra-estrutura.

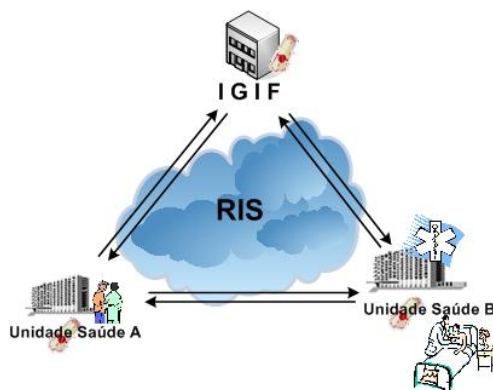
A infra-estrutura proposta baseia-se no uso de sistemas criptográficos assimétricos, ditos de "chave pública". Nestes sistemas, é atribuído a cada utilizador um par de chaves: uma chave a publicitar (pública) e uma chave a esconder (privada). A chave pública seria disponibilizada livremente em certificados digitais ou num directório de acesso público (por exemplo, na página *web* da instituição) e a chave privada deveria ser guardada em local de confiança do utilizador (por exemplo, no seu cartão de identificação profissional). Cada certificado digital (documento electrónico) teria o seu conteúdo reconhecido como verdadeiro mediante a assinatura digital, e ele aposta, isso seria feito pela autoridade certificadora (o IGIF, como aqui sugerido, ou uma outra entidade institucional de confiança). Tal autoridade representa um papel muito importante em termos da credibilidade da informação que transita na rede, pois possibilita a criação de uma relação de confiança entre parceiros intervenientes nas relações de prestação de cuidados de saúde.

[68] PKI – Public Key Infrastructure. Esta infraestrutura baseia-se no uso de sistemas criptográficos assimétricos.

Figura 20 – Triângulo de Confiança da PKI na Saúde

A autoridade certificadora é o vértice superior do triângulo de confiança necessário para o estabelecimento de sessões seguras na rede (ver Figura 20). Cada uma das partes representadas pelos vértices da base do triângulo confia na autoridade certificadora, e como estão por ela certificadas, podem criar sessões seguras de troca de informação.

A estrutura disponibilizada pela RIS ao nível das redes locais e servidores, não permite, por si só, dar resposta às necessidades de segurança. Implementar uma PKI requer a sua integração na infra-estrutura já existente e o uso de ferramentas apropriadas (gestor de correio electrónico, navegador web, etc.).

Como já foi referido, tipicamente, as redes locais que integram a RIS apresentam alguns elementos comuns: em geral as instituições estão protegidas por *firewall* própria ou com filtros de acesso (baseados em ACLs[69]) nos equipamentos de interligação (*routers*) e os servidores de *web* e correio electrónico encontram-se em zonas desmilitarizadas (DMZ).

Os serviços de correio electrónico e internet, em geral, são disponibilizados por uma plataforma em *Linux*, mas a interface com o utilizador é baseada no sistema *Microsoft Windows* (*Outlook* e *Internet Explorer, etc.).*

Estes serviços, para integrar a PKI, devem operar com o protocolo S/MIME[70] (adição de extensões de segurança ao formato de mensagem de correio electrónico MIME); opere como base de outros protocolos formando assim, SMTPS[71], POPS[72], IMAPS[73] e com um sistema de directório

---

[69] ACLs – Access Control List ou lista de controlo de acessos, lista que define quem tem permissões de acesso a certos serviços. Isto para que o servidor possa permitir ou negar acessos ou tarefas.

[70] S/MIME – Secure Multipurpose Internet Mail Extensions. Proporciona segurança no correio electrónico. Privacidade de conteúdo, integridade da mensagem, verificação do remetente e verificação do destinatário. Para mais especificações RFCs 2311 e 2312.

[71] SMTPS – Simple Mail Transfer Protocol Secure. Protocolo seguro usado no envio de correio electrónico através da internet.

[72] POPS – Post Office Protocol Secure. Protocolo seguro utilizado no acesso remoto a uma caixa de correio electrónico. RFC 1939.

[73] IMAPS – Interactive Mail Access Protocol Secure. Protocolo seguro em que as aplicações cliente consultam o correio no servidor não fazem o descarregamento para o computador local, toda gestão é efectuada no servidor. RFC 2060.

como o LDAP[74]. O navegador deve permitir a utilização de SSL/TLS e SET para comunicações e transacções seguras.

Para modelar esta infra-estrutura foram definidos os seguintes elementos (ver Anexo B): uma autoridade certificadora (CA[75]) do tipo subordinada; uma Sub CA; uma autoridade de registo (RA[76]); um sistema de directório público com acesso LDAP; uma impressora para o cartão profissional.

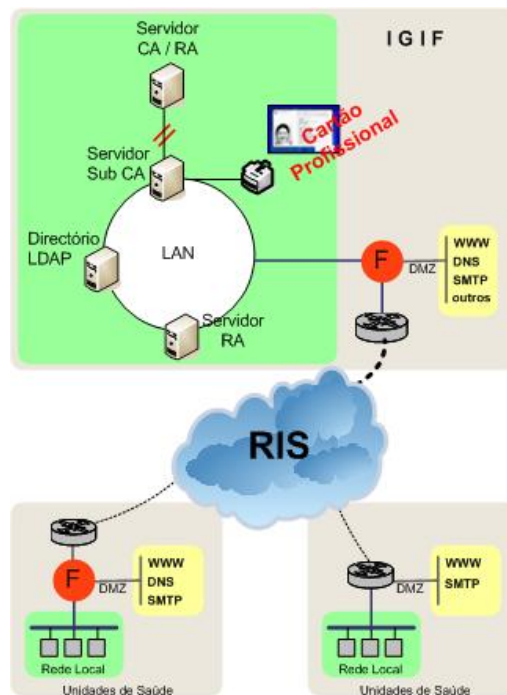



Figura 21 – Arquitectura de Implementação de uma PKI

A solução proposta assenta numa arquitectura do tipo centralizada, com duas vertentes:

- O IGIF é responsável pela emissão e gestão dos certificados institucionais (hospitais, centros de saúde, IGIF, etc.).
- As instituições são responsáveis pela gestão de todo o ciclo de certificação nas suas instituições (funcionam como Sub CAs). Estas acedem de uma forma segura a um servidor *web* disponibilizado pela RIS, partilhado por todas as instituições.

---

[74] LDAP – Lightweight Directory Access Protocol. É um protocolo para actualizar e pesquisar directórios através de TCP/IP. Um directório LDAP geralmente segue o modelo X.500. Mais especificações ver RFC 4210.

[75] CA – Autoridade Certificadora, é a entidade respondível pela emissão e administração dos certificados digitais. O CA actua como sendo o agente de confiança na PKI.

[76] RA – Autoridade de Registo, é responsável por guardar e verificar toda a informação que a CA precisa para emitir o certificado.

Os servidores de CA e RA ficam colocados na rede interna do IGIF protegidos pelos mecanismos de segurança já implementados na rede. Nesta rede também se propõe colocar o serviço de directório LDAP, cujas funções principais são a publicação de certificados e a publicação das listas de revogação respectivas.

O facto de existirem Sub CAs, permite que a CA do MS possa ser colocada em *off-line* e colocada num local físico seguro, aumentando a segurança do topo da hierarquia da PKI no MS. Uma medida sensata, pois caso a CA seja comprometida, coloca em causa toda a estrutura, obrigando a que seja refeita.

O pedido de emissão ou revogação de certificados digitais (ver, Anexo B) para servidores ou utilizadores é efectuado pelas instituições mediante o acesso seguro a uma aplicação *web* disponibilizada na RIS, através do preenchimento de um formulário com os dados identificativos do funcionário (nome do titular, nº BI, instituição onde trabalha e departamento, categoria profissional, etc.). De seguida, o departamento do IGIF responsável pela gestão de certificados digitais procede à emissão dos certificados e do respectivo cartão de identificação profissional para o caso do profissional de saúde, a sua identificação é única no sistema. Para além de imprimir a face do cartão, grava a chave privada no *chip* do cartão protegido por senha.

O uso de um *smart card* na identificação profissional associado ao uso de técnicas biométricas (por exemplo, impressão digital e leitura da íris) permitiria um aumento significativo do nível de controlo de acessos (por exemplo, poderia ser usado em funções normais de identificação, no controlo de portas, identificação e autenticação no sistema de informação clínico): tal cartão seria intransmissível (em caso de extravio nunca poderia ser usado por terceiros) e o seu cancelamento poderia ser feito de imediato; quando o utilizador abandonasse o posto de trabalho, obrigatoriamente teria de se fazer acompanhar do respectivo cartão, pelo que o *logout* seria automático e inevitável. No caso de tal cartão incluir também tecnologia RFID[77] a sua utilização seria extremamente cómoda, pois o profissional de saúde não teria sequer necessidade de o retirar do seu local de fixação, bastando para o efeito estar a uma distância não superior a 60 cm do respectivo leitor.

Considerando a crescente mobilidade dos profissionais de saúde (quer entre instituições que integram o MS ou não), a questão da identificação e autenticação, poderia ser resolvido da seguinte maneira, como cada uma das instituições de saúde faz a gestão da lista de atribuição de permissões de acesso aos seus sistemas, os profissionais de saúde podem ser autenticados e identificados em diferentes unidades de saúde usando o seu cartão de identificação e profissional. E como em última

77 RFID - Radio Frequency Identification.

instância os certificados são garantidos pela autoridade certificadora do MS estabelece-se uma relação de confiança.

Os certificados digitais devem ser periodicamente renovadas para incrementar a segurança (por exemplo, poderão ser válidos por um período de 5 anos), excepto em situações irregulares ou de desvinculo do funcionário, em que as instituições podem entender revogar. Os certificados devem ser actualizados antes de expirarem, para se evitar interrupções de serviço. Idealmente a actualização seria realizada automaticamente: sempre que a data de expiração estivesse próxima, ocorreria uma operação de renovação e um novo certificado seria gerado, que substituiria o anterior.

Em todo este processo é importante que todas as máquinas tenham os seus relógios internos sincronizados. O serviço *Timestamping* (ou serviço de selos temporais e notariado) (ver, Anexo B) é um serviço especial que confirma a recepção de documentos digitais numa data específica. É, portanto, um processo que associa uma data/hora a um documento.

Em conclusão, cada elemento desta infra-estrutura de chaves públicas possui um par de chaves, e através da utilização de uma ou de outra, consegue-se garantir a autenticação, integridade, não -repúdio e confidencialidade da informação clínica.

5.3. Implementação das Propostas de Melhoria

A implementação das políticas definidas, que são essencialmente genéricas ou traduzem o campo de actuação da autora, contribuiria para clarificar a vida profissional e para melhorar a prática no dia a dia nas instituições de saúde.

Neste item serão apresentados dois exemplos do que poderia ser o procedimento para a gestão de senhas numa instituição de saúde pública e uma solução do que poderia ser uma programação da infra-estrutura de chaves públicas no ministério da saúde.

5.3.1. Procedimento para Gestão de Senhas

Como foi referido anteriormente, uma das principais preocupações de segurança é a gestão de senhas. Enquadrado no ponto 5.1.4, item “Controlo de Acesso Lógico” da política de segurança apresentada, este procedimento, tem por finalidade estabelecer orientações que deverão ser adoptadas no que se refere à gestão de senhas com vista a colmatar vulnerabilidades muito comuns. O procedimento foi elaborado de acordo com a norma EN 12251: 2004 – *Secure User Identification for Healthcare, Management na Security of Authentication by Password* (ver Anexo A).

No contexto do caso de estudo apresentado, conclui-se a existência de uma heterogeneidade de aplicações com diferentes regras de identificação e autenticação dos utilizadores, para além de que raramente existem procedimentos escritos para a gestão de senhas.

Algumas das orientações, que a seguir se apresentam foram já implementadas no ambiente de trabalho em que a autora se insere. Sugere-se, então, que o procedimento para a gestão de senhas deva:

1. Exigir a identificação (única) e autenticação dos utilizadores antes de qualquer interacção com o sistema;
2. Exibir uma mensagem de política informática no ecrã inicial de que o serviço só pode ser utilizado por utilizadores autorizados;
3. Suprimir o aparecimento dos caracteres da senha na altura da sua inserção para autenticação;
4. Limitar número de tentativas falhadas de *login* (por exemplo, 3 vezes);
5. Limitar o tempo de vida de uma senha (por exemplo, 6 meses);
6. Permitir a alteração da senha por parte do utilizador;
7. Notificar o utilizador de que o tempo de utilização da senha está a terminar;
8. Obrigar ao uso de senhas complexas: com mais de 6 caracteres (alfanuméricos);
9. Proibir a reutilização de senhas antigas;
10. Estabelecer um mecanismo para definir senhas temporárias para tarefas específicas de curta duração;
11. Proibir a partilha de senhas;
12. O sistema de controlo de acesso deve solicitar nova autenticação após certo tempo de inactividade da sessão *(time-out)*;
13. Gerir informação (identidade) dos utilizadores activos;
14. Permitir a criação de estatísticas de *login*;
15. Garantir o armazenamento seguro de senhas (cifradas).

Para ser possível a concretização destas medidas foi desenvolvido um grande esforço ao nível da sensibilização e formação dos diferentes grupos profissionais, pois como já referido, uma das mais perigosas ameaças que afecta aos sistemas de informação na saúde advém do descuido dos próprios funcionários. Outra tarefa muito importante foi a reestruturação e uniformização das aplicações tendo em vista a implementação das políticas estabelecidas.

A uniformização das políticas ao nível da identificação e autenticação do utilizador, irá conduzir à construção de uma plataforma de acesso único às diferentes aplicações, tendo em vista um único ponto de acesso ao sistema de registo clínico do paciente.

5.3.2. Modelação, Programação e Implementação da PKI na Saúde

A proposta a seguir apresentada está próximo do que poderia ser uma solução a adoptar pelo IGIF na programação, implementação e operacionalização de uma infraestrutura de chaves públicas na saúde.

Para a programação da infra-estrutura de chaves públicas poder-se-á recorrer a acordos de licenciamento de *software* entre o IGIF e (Microsoft, Oracle em empresas informáticas relevantes) e/ou recorrendo a ferramentas "*Open Source*", que tornariam possível a construção desta infra-estrutura aproveitando recursos existentes e dispensando grandes investimentos. Como mera ilustração, do que seria possível fazer, refiro aqui um trabalho desenvolvido no âmbito deste mestrado na cadeira de Segurança em Sistemas e Redes, no qual colaborei, cujo objectivo era programar, configurar e testar uma PKI X.509 (Trabalho 5) [121].

A solução poderá ser desenvolvida com recurso a ferramentas disponibilizadas pelo OpenSSL [122], que fornece todas as ferramentas necessárias para a criação de uma PKI (funções de geração, revogação e exportação de chaves privadas e certificados). Para a programação da base de dados poderão ser utilizadas também ferramentas "*Open Source*". O serviço deverá ser disponibilizado na RIS via *web*, com recurso, por exemplo, ao servidor *Apache* em plataforma *Linux*.

De seguida é apresentado um conjunto de quadros relacionados com a interface de utilização e administração desta infra-estrutura. Os acessos ao servidor para gestão de certificados digitais são autenticados, por perfil e através de protocolo seguro (HTTPS).

Aplicação Web CA

Página principal da solução (Figura 22), distribuição segura do certificado CA de cada instituição e distribuição da lista de certificados revogados do MS. O IGIF é o gestor responsável pela gestão dos certificados digitais institucionais.

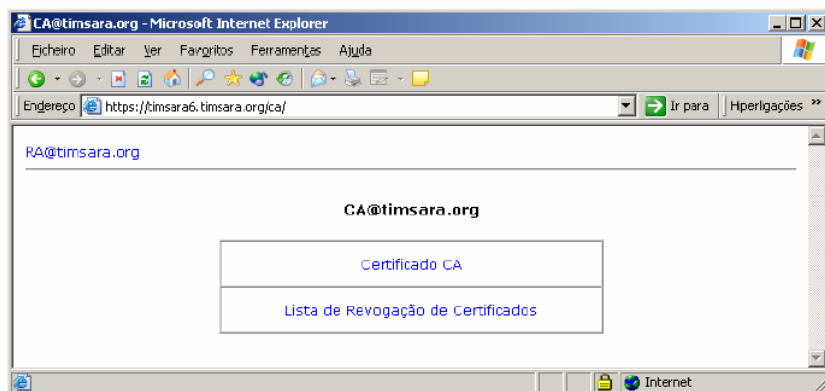



Figura 22 – Aplicação Web CA

Aplicação Web RA

Página principal da aplicação RA (Figura 23), acesso à gestão de identidades digitais onde os gestores institucionais podem gerar os certificados digitais para os seus utilizadores e servidores.

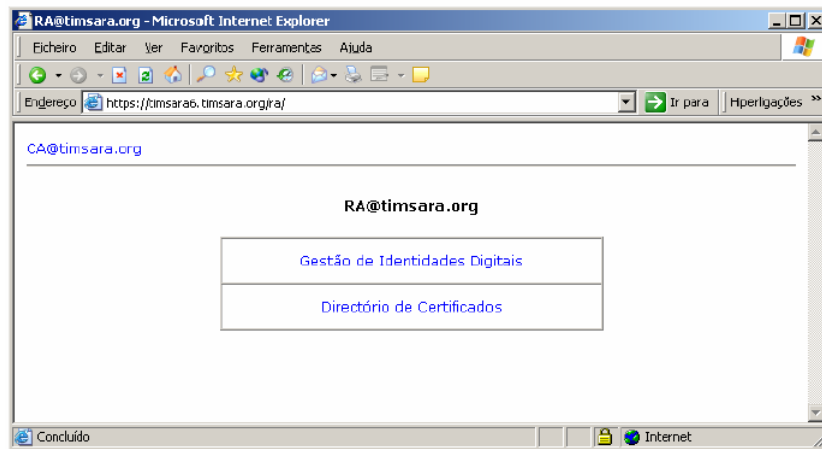



Figura 23 – Aplicação Web RA

A opção Gestão de Identidades Digitais permite aos gestores institucionais o acesso ao seu perfil e a gestão dos certificados dos seus utilizadores e servidores. No caso do gestor IGIF tem acesso à opção administração do CA.

Na opção Geração de Certificados Digitais de Utilizador (Figura 24), o gestor institucional pode gerir os certificados para os seus utilizadores.

Criação/Edição de Entidades@timsara.org - Microsoft Internet Explorer
Ficheiro Editar Ver Favoritos Ferramentas Ajuda
Endereço https://timsara6.timsara.org/ra/gid/addent.php?ses=eJxNjFEOwyAMQ++SE4RAAkkPMwUK(
Ir para
Hiperligações
CA@timsara.org RA@timsara.org Gestão de Identidades Digitais@timsara.org
Criação/Edição de Entidades@timsara.org
Utilizador:
Password:
Organização:
Area:
Nome:
Mail:
Perfil: Utilizador
Gravar
Concluído
Internet
Geração de Certificados de Utilizador@timsara.org - Microsoft Internet Explorer
Ficheiro Editar Ver Favoritos Ferramentas Ajuda
Endereço https://timsara6.timsara.org/ra/gid/gercerutil.php?ses=eJxNi0OOAiEMRu/CCQp0gHYOY9oO:
Ir para
Hiperligações
CA@timsara.org RA@timsara.org Gestão de Identidades Digitais@timsara.org
Geração de Certificados de Utilizador@timsara.org
Certificado para Paulo Monteiro emitido !
Atenção: palavra-passe para a chave privada = 471228027
Download: Certificado+ChavePrivada em formato PKCS#12 (.p12)
Concluído
Internet

Gestão de Utilizadores@timsara.org - Microsoft Internet Explorer
Ficheiro Editar Ver Favoritos Ferramentas Ajuda
Endereço https://timsara6.timsara.org/ra/gid/gestusers.php?ses=eJxNjFEOwyAMQ++SE4RAAkkPMwL
Ir para
Hiperligações
CA@timsara.org RA@timsara.org Gestão de Identidades Digitais@timsara.org
Gestão de Utilizadores@timsara.org
Gestão de Certificados de Utilizador
Todos os utilizadores
OK
Utilizador
Nome
Certificados
joe
Joe Doe
0
pmonteiro
Paulo Monteiro
2
saraujo
Sara Araujo
0
vbatista
Valentim Batista
2
Adicionar utilizador
Internet

Figura 24 – Gestão dos certificados de utilizador

Na opção <u>Geração de Certificados Digitais de Servidores</u> (Figura 25), o gestor institucional pode gerir os certificados para os seus servidores.

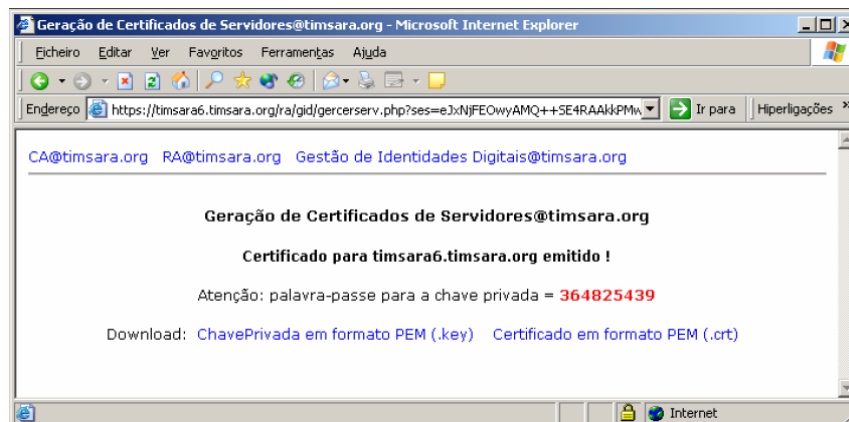
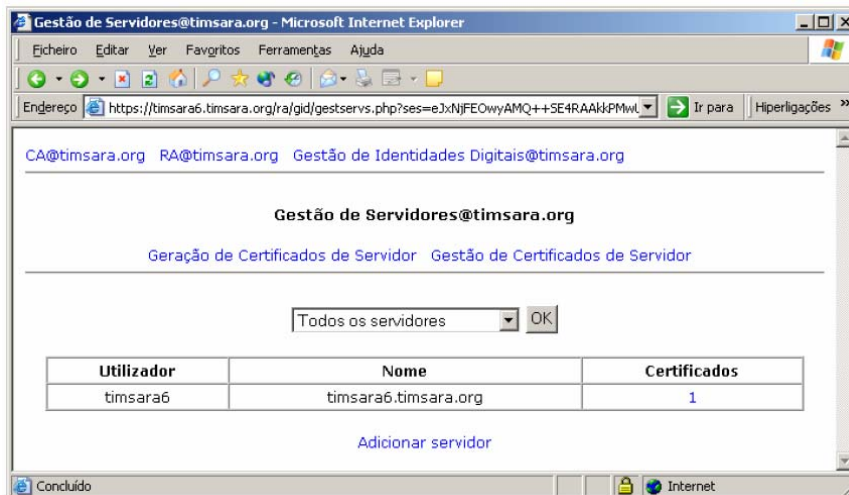
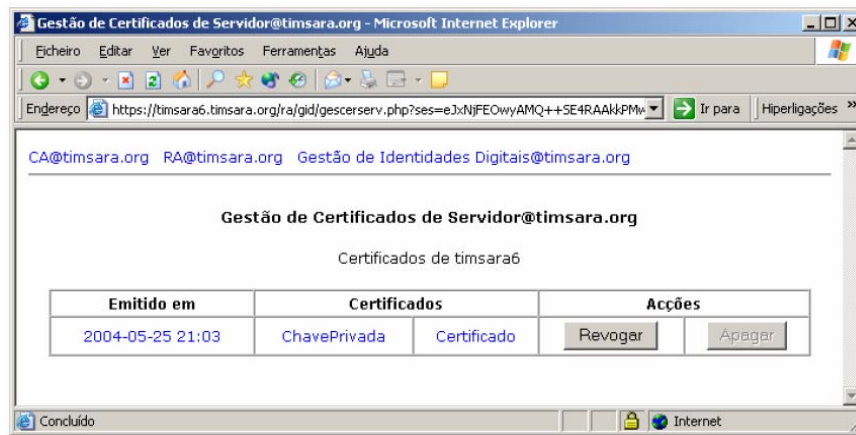



Figura 25 – Gestão de certificados digitais para servidores

O Directório Publico de Certificados Digitais dos Utilizadores que integram o Ministério da Saúde publicado na página do IGIF.

Esta é apenas uma proposta de implementação com recurso a ferramentas abertas (por exemplo OpenSSL), pouco dispendiosa do ponto de vista de investimento em desenvolvimento e tecnologia. Não é necessário aquisição de certificado *"root CA"* a uma empresa externa (Multicert, Verisign, etc.), pois este é disponibilizado pela ECEE. A dificuldade não está propriamente na sua programação, mas sim na sua implementação.

5.4. Conclusão

A implementação de uma infra-estrutura de segurança e de políticas de segurança é hoje um factor imprescindível ao desenvolvimento e implementação de sistemas que permitam criar um registo clínico único e em formato electrónico.

A abertura das barreiras à informação nas instituições clínicas pressupõe, como requisito fundamental, que exista um trabalho prévio de estruturação interna nos sistema de informação de forma a dotá-los com mecanismos seguros de identificação e autenticação dos utilizadores, impondo o uso da assinatura digital impedindo o "não repúdio" dos actos dos profissionais de saúde, e garantindo confidencialidade e integridade dos dados.

Assegurados que estejam estes pontos, os sistemas de informação clínicos estão em condições de permitir o acesso e partilha de informação remota recorrendo a estruturas de confiança, permitindo, inclusivamente, a sua integração numa estrutura regional, nacional ou mesmo internacional.

Com estas propostas poderemos dotar os sistemas de informação clínicos com um processo de autenticação forte e seguro, permitindo a sua inserção numa rede alargada de confiança,

utilizando as mesmas tecnologias de segurança dos sistemas em ambientes *web-based*. Desta forma o acesso remoto e partilha da informação clínica, sobre os sistemas existentes e de forma segura, poderia ser implementado recorrendo às mesmas tecnologias (certificados digitais, PKI, TTPs[78], cartões inteligentes), quer os acessos sejam provenientes da intranet ou do exterior da instituição (por exemplo, RIS).

Não existem soluções de segurança perfeitas ou completas, exige-se uma melhoria contínua. Um factor relevante sobre a segurança das tecnologias e sistemas é a definição de políticas de segurança, a escolha de equipamentos e de sistemas de qualidade e bom planeamento da infra-estrutura de rede.

Em resumo, todas as propostas apresentadas têm por finalidade estabelecer orientações genéricas que poderão ser adoptadas pelas organizações e deverão ser embebidas noutros processos a elas específicos, com o principal objectivo de colmatar as principais vulnerabilidades identificadas na gestão e utilização da informação clínica.

[78] TTPs – Trusted Third Parties. Serviços externos destinados a facilitarem as relações de confiança envolvidas nas comunicações.

6 CONCLUSÕES FINAIS

O desenvolvimento contínuo das tecnologias de informação e a sua utilização crescente na saúde e em todos os outros sectores de actividade tem consequências importantes na segurança e mobilidade da informação. A evolução para cenários de troca segura de mensagens electrónicas entre instituições induz ganhos significativos de produtividade e optimização dos processos de prestação de cuidados de saúde. Assim como a colaboração entre instituições pode ser suportada por tecnologias de informação, também os cuidados médicos beneficiam de uma integração dos sistemas e processos. O processo clínico deve então evoluir para um formato electrónico e ser entendido já não só como uma memória escrita da prestação de cuidados, mas como um contexto de colaboração entre múltiplos serviços e profissionais, intra-instituição e inter-instituições.

O registo clínico electrónico, para além de conter informação clínica do paciente, deve mostrá-la de forma integrada. Por um lado as fontes de informação que contribuem para o processo clínico electrónico são diferentes, usam diferentes tecnologias e diferentes formatos. Por outro lado a forma de visualização da informação clínica deverá poder ser organizada conforme as necessidades de cada utilizador.

Também se reveste de muita importância a questão que está associada à utilização de normas nacionais e internacionais que permitam a circulação e interoperabilidade de registos electrónicos entre várias instituições, para além do respeito pelos princípios éticos e questões legais associadas.

Os profissionais de saúde trabalham num ambiente social e, como tal, as suas acções são também sujeitas a princípios que correspondem a outros tantos direitos de cidadania. Os mais estreitamente ligados com a segurança da informação são o princípio da privacidade e o princípio da integridade. Todas as pessoas têm o direito fundamental à privacidade e, por isso, ao controlo sobre os seus dados pessoais (por exemplo: na sua recolha, armazenamento, acesso, uso e transmissão). Para além disto, o direito à integridade exige que os dados que tenham sido recolhidos devem ser protegidos contra a perda, corrupção, destruição, e alteração indevidas ou não autorizadas.

A constante evolução das tecnologias na saúde tem provocado um aumento do uso de sistemas de informação por parte dos profissionais de saúde. A quantidade de dados armazenada em bases de dados clínicos, bem como o acesso a estas, tem vindo a aumentar face à generalização das redes de computadores não só dentro de cada instituição mas também entre diferentes instituições da saúde. Isto é ainda mais notório com a introdução de novas tecnologias, como as redes sem fios, onde o acesso à Internet e a bases de dados *online* é cada vez mais independente do local físico de onde é efectuado.

Cada vez mais as instituições de saúde estão dependentes do funcionamento permanente dos seus sistemas de informação, o que implica a necessidade de mais acções com o intuito de diminuir a probabilidade de interrupções nos serviços de forma a garantir a sua permanente disponibilidade.

A segurança das redes e da informação tornar-se-á, muito provavelmente, um elemento chave no desenvolvimento da sociedade da informação, dado que a ligação em rede desempenha um papel económico e social crescente. O risco associado é também crescente, pois além da maior exposição da informação sensível, os danos causados por um potencial ataque bem sucedido são também maiores.

A segurança das redes e da informação é uma questão dinâmica, o ritmo das mudanças tecnológicas gera continuamente novos desafios, os problemas de ontem desaparecem e as soluções de hoje já não fazem sentido. O mercado oferece quase diariamente novas aplicações, serviços e produtos que devem ser triados e escolhidos para utilização, caso mostrem ser seguros. No entanto, alguns processos constituirão sempre desafios significativos para uma politica de segurança global, pelo que o esforço com a segurança deve ser contínuo.

A análise da situação actual dos sistemas de informação clínica em Portugal (ver Capítulo 3), mostra que não estão definidas políticas e mecanismos de segurança adequados ao nível de todo o SNS. Outros problemas identificados que podem ameaçar a seguranças dos sistemas de informação clínica têm a ver com as tecnologias obsoletas em uso, a não integração dos sistemas e o comportamento não adequado dos utilizadores.

Com o objectivo de poder contribuir para a melhoria da situação de segurança dos sistemas de informação clínica em Portugal foi proposto uma infra-estrutura de segurança e políticas comuns às instituições que integram o Ministério da Saúde (ver Capítulo 5). Uma infra-estrutura de chaves públicas é considerada como um bom instrumento para a obtenção de um maior nível de protecção.

Para além dos mecanismos e políticas, referido anteriormente é fundamental não descurar a actualização dos sistemas, sua integração, formação e sensibilização dos utilizadores.

Há que proteger a privacidade de um paciente e este tem de confiar na organização onde é tratado e onde confia a guarda dos seus dados pessoais. É impossível garantir uma segurança a 100%, no entanto é possível reduzir os riscos ou restringir possíveis danos devido à má utilização ou ao uso abusivo.

Esta discussão poderia servir de ponto de partida para um estudo pormenorizado desta temática ou outros estudos específicos. Como trabalhos futuros, penso que seria um contributo importante para os sistemas de informação clínica em Portugal, sem esquecer as questões de segurança, efectuar uma análise aprofundada e a apresentação de propostas concretas relativas aos seguintes pontos:

- políticas e privilégios de acesso e manipulação da informação clínica por perfil de utilizador, i.é., quem deve aceder e a que dados podem aceder;
- arquitectura de uma PKI adequada à saúde;
- arquitectura para o registo clínico único do paciente em Portugal (Processo Clínico Electrónico Único) – estudo de casos, legislação, normalização e arquitectura;
- estratégias e políticas pormenorizadas para os sistemas de informação da saúde em Portugal, tento como referências casos de sucesso no mundo;
- normalização e compatibilização dos sistemas de informação clínica em Portugal com tecnologias e normas internacionais na área da saúde (como o HL7 e, especialmente, o HIPAA);
- implementação do VoIP na RIS de forma segura e com garantias de QoS;
- reestruturação dos sistemas de informação clínica com vista à utilização massiva de soluções móveis;
- alteração da legislação que regula os dados clínicos no sentido de dar resposta às necessidade actuais.

GLOSSÁRIO

IPsec – Internet Protocol Secure. O protocolo IPsec oferece para ambientes TCP/IP mecanismos de segurança (autenticação e encriptação) ao nível IP. Para mais informação RFC 2401.

Anti-spam – O termo SPAM é usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. O uso se filtros anti-spam permite filtrar a entrada desses e-mails não desejados.

Antivírus – Os programas de antivírus fazem análise de arquivos disseminados pela Internet ou correio electrónico tentando neles detectar código malicioso.

ARP – Address Resolution Protocol. O protocolo TCP/IP relaciona dinamicamente um endereço IP (endereço lógico) com um endereço MAC (endereço físico). O ARP é usado dentro de um segmento de rede e é limitado a redes que suportam broadcast.

ATM – Asynchronous Transfer Mode. Uma rede baseada num conjunto de *switches* ATM inter-conectados por ligações ATM ponto-a-ponto em fibra óptica. Esta tecnologia introduz o conceito de células, endereçamento e circuitos virtuais.

Certificados Digitais – Um certificado digital pode ser definido como um documento electrónico, assinado digitalmente por uma terceira parte confiável, que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

DMZ - DeMilitarized Zone ou "Zona Neutra" corresponde ao segmento, parcialmente protegido, que se localiza entre redes protegidas e redes desprotegidas e que contém todos os serviços e informações para clientes ou públicos.

DNS – Domain Name System. O serviço DNS permite que as máquinas na rede sejam identificadas por um nome, para além da identificação pelo endereço IP.

Firewall – Um firewall ou barreira “corta fogo” é um equipamento colocado na zona fronteira de uma rede, cujo o principal objectivo é o controlo de acessos não autorizados oriundos de outras redes, por exemplo, a Internet. Especificado pelo RFC 2828.

IDS – Intrusion Detection System. Sistema de detecção de intrusão, é definido como sendo um serviço que monitora e analisa eventos de uma rede e providencia alertas em tempo real de acessos aos recursos da rede não autorizados. Para mais informação ver o RFC 2828.

Kerberos – É um protocolo de autenticação especificado no RFC 1510.

MAC – Media Access Control. Protocolo de baixo nível, implementado em hardware, usado para acesso à rede. O termo MAC address é geralmente usado como sinonimo de endereço físico.

Proxies – Firewalls de aplicação ou simplesmente *proxies*, todo o tráfego interno ou externo à rede é encaminhado para o proxie, que funcionando ao nível de aplicação, pode executar funções de autenticação, controlo de acesso, etc.

Router – O router ou encaminhador é um dispositivo para interligação de redes de diferentes tecnologias que fazem o encaminhamento e a comutação dos pacotes entre si.

SET – Secure Electronic Transactions. É um conjunto de protocolos e mecanismos de segurança que permite a realização de transacções seguras com cartão de crédito através da internet.

TCP/IP – Transmission Control Protocol / Internet Protocol. È uma solução tecnológica usada em redes privadas e de telecomunicações como suporte computacional para um grande número de aplicações, para o desenvolvimento, como plataforma de interconexão e operação de Internet.

Telnet – Protocolo pertencente ao TCP/IP, que permite o acesso remoto via Internet a um outro computador. Por meio de um login e uma senha.

Token – Dispositivo físico ou um testemunho, geralmente ligado à porta USB do computador, armazena as chaves privadas e os certificados digitais, para além da identificação e autenticação permite a validação do utilizador.

VLANs – Virtual Local Area Network. Uma rede local virtual, é uma rede logicamente independente. Várias VLANs podem coexistir em um mesmo comutador (switch). Um outro propósito de uma rede virtual é restringir acesso a recursos de rede. Uma VLAN geralmente é configurada para mapear directamente uma rede ou sub-rede IP. Ligações switch a switch e switch a router são chamados de troncos e servem de espinha dorsal entre o tráfego que passa através de diferentes VLANs.

VPN – Virtual Private Network. Definida pelo RFC 2828 como sendo uma conexão de computadores de uso restrito, que se estabelece sobre uma estrutura física de uma rede pública, como por exemplo a internet.

SSL – Secure Socket Layer. O protocolo SSL mantém a segurança e integridade do canal de transmissão através da Internet, em conexões do tipo TCP, usando cifragem, autenticação e mensagens com código de autenticação.

REFERÊNCIAS

		Descrição	Último Acesso
[1]	http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_pt.pdf	Documento eEuropa 2005.	Dez-05
[3]	http://www.di.fc.ul.pt/tech-reports/03-27.pdf	Implementação de uma PKI no Ministério da Justiça	Nov-05
[4]	http://www.rederio.br/downloads/pdf/atm.pdf	Tutorial Redes ATM.	Nov-05
[5]	http://www.dem.ubi.pt/~humberto/Investiga/ARTIGOS/Redes_Sem_Fios_IEEE_802_11_Instalacao,_Configuracao_e_Seguranca.pdf	Instação e configuração de redes sem fios	Nov-05
[11]	http://www.ordemdosmedicos.pt/ie/institucional/CNE/b5.htm	Código deontológico destinado a médicos.	Out-05
[12]	http://www.abpi.org.uk/links/assoc/pmcpa.asp	Regulação dos aspectos de prescrição de medicamentos.	Out-05
[13]	http://www.healyprozac.com/MCA/default.htm	Entidade governamental, no Reino Unido, trabalha na regulação dos aspectos de prescrição de medicamentos	Out-05
[14]	http://www.hon.ch/	Regras definidas pelo HONcode.	Out-05
[15]	http://www.ihealthcoalition.org/ethics/code0524.pdf	Princípios definidos pelo IHCC Code.	Out-05
[16]	http://www.imia.org/pubdocs/rec_english.pdf/	Código de ética para os profissionais na área IM.	Out-05
[17]	http://www.cnpd.pt/index.asp	Homepage Comissão Nacional Protecção de Dados.	Out-05
[18]	http://www.cnpd.pt/bin/legis/nacional/lei_6798.htm	Lei da Protecção de Dados Pessoais, Lei nº67/98 de 26 de Outubro.	Out-05
[19]	http://www.nema.org	Norma DICOM	Set-05
[20]	http://medical.nema.org/dicom/2004/04_15PU.PDF/04_15PU.pdf	Aspectos de gestão segurança norma DICOM	Set-05
[21]	http://www.hl7.org	Especificações norma HL7	Set-05
[22]	http://www.microsoft.com/biztalk/default.mspx	Norma HL7	Set-05
[23]	http://www.centc251.org	Normas do grupo detrabalho nº 251 CEN	Set-05
[24]	http://www.ramit.be/semric/	Projecto SEMIREC Segurança nos registos médicos e comunicaçõe	Set-05
[25]	http://www.iso.org	Organização Internacional de Normalização.	Set-05
[26]	http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=4720&scopelist=PROGRAMME#top	Lista as normas associadas ao grupo de trabalho TC 215 no domínio Health Informatics.	Jan-06
[31]	http://www.omg.org	Técnologia CORBA	Set-05
[32]	http://healthcare.omg.org/	Técnologia CORBA	Set-05
[33]	ftp://ftp.omg.org/pub/docs/formal/98-12-17.pdf	Técnologia CORBA	Set-05
[34]	http://www.omg.org/technology/documents/formal/omg_security.htm	Técnologia CORBA	Set-05

[35]	http://www.hipaa.org/	Site Health Insurance Portability Accountability Act of 1996.	Set-05
[36]	http://www.thetechdictionary.com/term/hipaa_compliance	Tech Dictionary HIPAA	Set-05
[37]	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2003_register&docid=fr20fe03-4.pdf	Norma de segurança.	Set-05
[38]	http://aspe.hhs.gov/admnsimp/	Regras HIPAA.	Set-05
[39]	http://www.cms.hhs.gov/HIPAAGenInfo/04_PrivacyStandards.asp#TopOfPage	U.S Department od Health & Human Services.	Set-05
[40]	http://aspe.hhs.gov/admnsimp/pl104191.htm	Public Law 104-191 Aug 21 1996 (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996)	Set-05
[41]	http://www.ieee.org	Normas de segurança IEEE	Set-05
[42]	http://www.finn.pl/xml/komputeryzacja/sprawozdawczosc/iso9735	Listagem das partes que constitui a norma EDIFACT	Dez-05
[43]	http://www.astm.org/cgi- in/SoftCart.exe/COMMIT/COMMITTEE/E31.htm?E+mystore	Normas ASTM	Set-05
[44]	http://www.cpri.org/docs/docs.html	Normas CPRI	Set-05
[45]	http://www.iso-17799.com/	Directório de informação sobre a norma ISO 17799.	Set-05
[46]	http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html	Informação sobre o status da norma.	Set-05
[47]	http://www.callio-pt.com/	Disponibiliza software de apoio ás organizações para implementar o padrão BS 7799 / ISO 1799.	Set-05
[48]	http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=85	Um pouco historia da norma ISO/IEC 17799.	Fev-06
[49]	http://www.checkuptool.com.br/artigo_11.htm	Descreve algumas das alteração entre ISO/IEC 17799: 2000 e ISO/IEC 17799: 2005.	Fev-06
[50]	http://www.checkuptool.com.br/PDF/NBR_ISO17799.pdf	Mapa comparativo entre ISO/IEC 17799: 2000 e ISO/IEC 17799: 2005.	Fev-06
[51]	http://www.sis.pt/auxiliar/segnac4.htm	Normas para a segurança nacional, salvaguarda e matérias classificadas, Segurança Informática – SEGNAC 4.	Fev-06
[52]	http://www.ukerna.ac.uk/	Papel branco descrevendo o estado da criptografia H.323.	Fev-06
[53]	http://www.videnet.gatech.edu/cookbook.pt/list_page.php?topic=4&url=wireless.html&level=1&sequence=1&name=Wireless%20e%20Vídeo%20Satélite	Videoconferência sobre redes sem fios.	Nov-05
[54]	http://www.medis.or.jp/2_kaihatu/iso/iso_tc215_wg5/data/b3_iso_dis_21549-2_e.pdf	Norma ISO/DIS 21549	Fev-06
[55]	http://www.portugal.gov.pt/Portal/PT/Governos/Governos_Constitucionais/GC17/Ministerios/PCM/MP/Comunicacao/Outros_Documentos/20051006_MP_Doc_ECEE.htm	Constituição da Entidade Cerificadora Electrónica Estado.	Fev-06
[59]	http://www.igif.min-saude.pt	Home page do Instituto de Informática e Gestão Financeira do SNS.	Jan-06
[67]	http://www.alert.pt/?&sel_men=211	Homepage da empresa MNI, principal produto na área da saúde	Jan-06
[68]	http://www.alert-er.com/index.php?multiplo=1	Descrição da aplicação ALERT®.	Jan-06
[69]	http://www.who.int/classifications/icd/en/	Classificação internacional das doenças.	Jan-06
[70]	http://www.committee-german-medicine.de/cms/front_content.php?idcat=169&idart=1707	DRG online.	Jan-06
[71]	http://www.health.gov.au/internet/wcms/publishing.nsf/Content/Casemix-1	Australian Government – Department of Health and Ageing, DRG.	Jan-06

[72]	http://www.nlm.nih.gov/mesh/presentations/tafumls/ppframe.htm	National Library of Medicine, National Institutes of Health,	Jan-06
[73]	http://www.cap.org	College of American Pathologists.	Jan-06
[74]	http://www.snomed.org	Site do sistema de classificação SNOMED.	Jan-06
[75]	http://www.sinaisvitais.pt/index.php?option=com_content&task=view&id=134&Itemid=49&limit=1&limitstart=1	Um exemplo de telemonitorização	Jan-06
[76]	http://www.cipe.org/	Classificação Interncional das Práticas de Enfermagem	Dez-06
[79]	http://www.e-projects.ubi.pt/samurai/	Homepage do projecto SAMURAI.	Dez-06
[80]	http://www.it.pt/project_detail_p.asp?ID=501	Homepage do Prof. Fernando J. Velez responsável pela implementação do projecto WiMAX.	Jan-06
[81]	http://www.e-ojects.ubi.pt/wimax/txt/05_10_04_Workshop_IPMovel_RWimax.pdf	Projecto rede sem fios Centro Hospitalar Cova da Beira.	Jan-06
[82]	http://www.ieeta.pt/rtsaude/Home.php	Homepage do projecto Rede Telemàtica da Saúde.	Jan-06
[83]	http://www.ieeta.pt/rtsaude/docs/RTS_RT_1_1_1_SumExec_V1_0.pdf	Relatório de Análise de Processos e Fluxos de Informação.	Jan-06
[93]	http://www.cnpd.pt/bin/relatorios/outros/Relatorio_final.pdf	Relatório "Auditoria ao tratamento de informação de sáude nos Hopsitais"	Dez-06
[94]	http://www.openehr.org/	Fundação para o PCE.	Fev-06
[95]	http://www.centis.pt/Prorec_pt/ProrecTop.htm	Centro PROREC em Portugal.	Fev-06
[96]	http://www.eurorec.org/	Centro Europeu de registos clínicos electrónicos.	Fev-06
[97]	http://www.portaldasaude.pt./portal	Portal da Sáude Português	Fev-06
[98]	http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_pt.pdf	Documento em pdf eEuropa 2005.	Fev-06
[99]	http://europa.eu/scadplus/leg/pt/lvb/l24226.htm	Documento em pdf eEuropa 2005.	Fev-06
[100]	http://www.videnet.gatech.edu/cookbook.pt/list_page.php?topic=2&url=telemed.html&level=2&sequence=2.1&name=Telemedicina	Telemedicina	Fev-06
[101]	http://www.videnet.gatech.edu/cookbook.pt/list_page.php?topic=4&url=wireless.html&level=	Videoconferência sobre redes sem fios.	Fev-06
[102]	http://www.dgsaude.pt/upload/membro.id/ficheiros/i007480.pdf	Recomendações para o Desenvolvimento da Telemedicina em Portugal.	Fev-06
[103]	Apresentação "Telemedicina Em Emergência", II Fórum Ibérico de Telemedicina, Viseu, Outubro 20006, Dr. Joaquim Cardoso.		Fev-06
[104]	http://www.haivision.com/downloads/CSCmas.pdf	Caso estudo de Telecirurgia.	Jan-06
[105]	http://eden.dei.uc.pt/eei2005/docs/apresentacoes/pdfs/MyHeart.pdf	Vencer as doenças cardiovasculares: a contribuição de engenharia.	Jan-06
[106]	http://www.philips.pt/PV_Article-16699.html	Empresa envolvida no projecto "Vencer as Doenças Cardiovasculares".	Jan-06
[107]	http://www.hitech-projects.com/euprojects/myheart/	Página do projecto MyHeart.	Jan-06
[108]	http://www.mobihealth.org/	Projecto que visa o desenvolvimento de novos serviços e aplicações na área da saúde móvel.	Jan-06
[114]	http://www.cartaodocidadao.pt/images/stories/relatorio_prova_conceito.zip	Relatório Prova do Conceito.	Jan-06
[122]	http://opengroup.org	Disponibiliza ferramentas para criar uma PKI.	Dez-05

[124]	http://www.sun.com/software/solaris/pam/	Módulo PAM da Solaris	Fev-06
[125]	http://www.softpanorama.org/Authentication/pam.shtml		Fev-06
[126]	http://www.fca.pt/livros-html/downloads/316_8asi_p2.pdf	Fases implementação de um Plano de Segurança.	Dez-05
[132]	http://www.ptinovacao.pt/noticias/2003/out%205atelemedic.htm	Telemedicina em cardiologia Pediatrica.	Out-05
[133]	http://www.ccr-norte.pt/outrosic/inteiiia.php	Página do programa ITERREG III.	Dez-05
[136]	http://www.jornaldoalgarve.pt/artigos.asp?varNumero=5087	Projecto Telemedicina Algarve.	
[138]	http://www.cnpd.pt/bin/legis/leis_nacional.htm	Legislação portuguesa relacionada com a protecção de dados	
[139]	http://www.ehto.org/		
[140]	http://www.med.kyushu-u.ac.jp/info/std/archives/cat_isotc215.html	Directório de standards na área Informática Médica	Fev-06
[141]	Engenharia de Redes Informáticas - Emundo Monteiro, Fernando Boavida. ISBN 972-722-203-X	Arquitecturas tecnologias e equipamentos; aspectos de gestão; metodologias e projecto.	Dez-05
[142]	MSc in Information Security - RHUL - September 2002, Ana Farreira	Aspectos de Segurança	Dez-05
[144]	http://www.unifr.ch/derechopenal/legislacion/pt/CPPortugal.pdf	Codigo Penal Português	Fev-06

Anexo A – Normas e Sistemas de Classificação e Codificação

1 Normas na Informática Médica

As organizações que se dedicam ao desenvolvimento de normas, assim como American Society for Testing and Materials (ASTM[79]), Health Level Seven (HL7), Object Management Group (OMG), o Computer-based Patient Records Institute (CPRI), Comité Européen de Normalization (CEN[80]), estudam e produzem normas relacionados com os aspectos de segurança dos sistemas de informação para a saúde através dos seus grupos de trabalho e de projectos especiais.

O foco de atenção destes grupos de trabalho é desenvolver politicas de segurança, procedimentos para lidar com as ameaças aos sistemas de segurança e também definir serviços de segurança.

Actualmente as normas de segurança mais usadas nos sistemas de informação para a saúde são: CEN TC 251 na Europa e o ASTM nos Estados Unidos. As organizações que não estão acreditadas para o desenvolvimento de normas, como Computer-based Patient Record Institute (CPRI) e CORBAmed a sua actividade passa por assistir e promover o processo de desenvolvimento de normas através da sua participação no ANSI-HISB (American National Standards Institute – Health Informatics Standards Board).

As várias organizações apresentam preocupações na harmonização das normas e cooperam entre si no seu desenvolvimento e promoção e baseiam as suas recomendações em técnicas ou mecanismos de protecção de uso geral.

A maioria das normas requer revisões periódicas, devido a evoluções tecnológicas, novos métodos ou materiais, ou novas exigências de qualidade e segurança, sendo usual uma revisão a intervalos não superiores a cinco anos.

Segue-se uma descrição sumária (ver Tabela 1) do conjunto de normas mais importantes do ponto de vista dos aspectos de segurança, e cujo objectivo é atingir a compatibilidade, modularidade e interoperabilidade entre sistemas heterogéneos na área da saúde.

---

[79] ASTM - American Society for Testing and Materials.

[80] CEN - Comité Européen for Normalisation.

Tabela 1 – Normas de Segurança na Área da Informática Médica

Nome	**Designação**	**Org**	**Âmbito** **Campo de Aplicação**	**Uso**	**Aspectos de Segurança**	**Especificação**	**Mecanismos de** **Segurança Propostos**
DICOM	Digital Imaging Communications in Medicine	NEMA	A norma DICOM define um conjunto de regras que permitem que imagens médicas e informações associadas sejam trocadas entre equipamentos de imagem, computadores e entidades ligadas ao sector da saúde.	Internacional	Part 15 – Security and System Management Profiles.	Especifica um conjunto de orientações referentes a perfis para gestão de sistemas e segurança.	-Protocolo TLS -Certificados Digitais (X.509) -Smartcards
HL7	Health Level Seven	ANSI	Protocolo para troca, manutenção e integração de dados relativos a pacientes. Aplicações clínicas: gestão de doentes, pedidos e resultados de exames e análises, registos de enfermagem e médicos, dietas, pedidos de farmácia, agendamento de consultas e actividades, reconhecimento de voz, sinais fisiológicos, lista de problemas dos pacientes, etc.	EUA Em expansão na UE	SIGSecure - Standard Guide for EDI (HL7) Communication Security. Standard Guide for Implementing EDI (HL7) Communication Security.	Endereçado para o desenvolvimento de transacções seguras HL7. Focaliza a atenção no uso do HL7 num ambiente de comunicações onde existe a necessidade de serviços de comunicações seguros como autenticação, encriptação, não repúdio e assinatura digital.	-Serviços externos de segurança - Terceira Parte de Confiança (TTPs - Trust Third Parties); -Chaves públicas ou infra-estruturas de chave simétrica; -Assinatura Digital; -Verificação do valor criptográfico; -Encriptação. -Segurança dos Protocolos de comunicação por camada do modelo OSI (TLS, IPsec, IPv6, SSL, SSH, SHTTP, SFTP, etc.) -Proposta de infra-estrutura de segurança forte PKI. Recomendado o uso de *chipcards* combinados com o código PIN e ou sistemas biométricos.
CEN/CT 251	Comité Européen Normalisation / Technical Committee 251	CEN	Tem por objectivo atingir a compatibilidade e interoperabilidade entre sistemas heterogéneos e implementar modularidade entre os sistemas de informação para a saúde.	UE	WGIII – Security, Safety and Quality.	Especifica um conjunto de normas de segurança: ENV 12924, ENV 12388, ENV 13608, etc.	- Define Politicas gestão Segurança; - Cartões de Identificação Electrónicos; - Cartões Profissionais de Saúde; - Assinatura Digital; - Certificados Digitais; - Selos temporais;
ISO/CT 215	International Standards Organization / Technical Committee 215	ISO	Normalização das tecnologias de comunicação necessárias para atingir a compatibilidade e interoperabilidade entre sistemas independentes na área da saúde.	UE	WG 4 – Security.	Definição de normas, de modo a assegurar confidencialidade, disponibilidade, integridade e responsabilidade, bem como os princípios gerais para a administração da segurança na área da saúde. ISO/TS 17090, ISO/WD 27799, ISO 22857, etc.	- Implementação PKI; - Guia para protecção de dados; - Guia para a gestão da segurança.
CORBA	Common Object Request Broker Architecture	OMG	CORBAmed define as tecnologias para a interoperabilidade dos sistemas de saúde. CORBAsec, especificações de segurança.		CORBAsec	Tecnologia orientada ao objecto. Desenvolvimento de funcionalidades de segurança: identificação, autenticação, delegação privilégios, confidencialidade, etc. Apresenta um modelo para a segurança dos objectos CORBA-Security.	ATLAS; CSIv2; CORBA security services PKI; RAD; SECP.
HIPAA	Health Insurance Portability and Accountability Act	USA	Define um conjunto de regras a seguir em planos de saúde.				

1.1 DICOM

A norma DICOM *(Digital Imaging Communications in Medicine),* DICOM 3.0: 2004 [19], tem sido desenvolvida para atender às necessidades de fabricantes e utilizadores de equipamentos de imagem médica.

A norma DICOM define um conjunto de regras que permitem que imagens médicas e informações associadas sejam trocadas entre equipamentos de imagem, computadores e entidades que actuam na área da saúde. Estabelece uma linguagem comum entre os equipamentos de marcas diferentes, que geralmente não são compatíveis, e entre equipamentos de imagem e computadores, estejam estes em hospitais, clínicas ou laboratórios geograficamente distribuídos. É uma especificação detalhada que descreve meios de formatação e transmissão de imagens e informações associadas.

Esta norma já é usada em Portugal por entidades que implementaram PACS (Picture Archiving Communication System), ou pelos sistemas de telemedicina existentes, e tem uma grande influência nos sistemas de informação das instituições de saúde pois, para além de disponibilizar as imagens através da rede, permite que se crie um arquivo digital de imagens, e assim se convirja para o PCR único (Processo Clínico Electrónico).

A adopção do norma DICOM pelos fabricantes de equipamentos de imagem médica abriu uma nova perspectiva sobre a qualidade dos serviços hospitalares, permitindo que os dados relativos ao utente sejam disponibilizados de uma forma rápida e segura em qualquer ponto da instituição ou do mundo.

A parte da norma PS 3.15 - Perfis de Segurança, especifica um conjunto de orientações referentes a perfis para gestão de sistemas e segurança, no documento *Part 15: Security and System Management Profiles* [20].

Em sistemas que usam a norma DICOM como protocolo de comunicação, perfis para gestão de sistemas de segurança são definidos por referenciais externos e normas existentes, tais como TLS[81], ISCL, DHCP[82] e LDAP[83]. Estes referenciais utilizam técnicas de segurança como chaves públicas e *smart cards*. A encriptação dos dados pode usar vários esquemas normalizados de encriptação.

No âmbito do campo de aplicação, esta norma providencia mecanismos que possam ser usados para implementar uma politica de segurança tendo em atenção a comunicação de objectos DICOM entre aplicações. Esta norma assume que para estabelecer acessos seguros às aplicações é usado o protocolo TLS e certificados digitais. Adicionalmente os certificados são validados através de

---

[81] TLS - Transport Layer Security.

[82] DHCP - Dynamic Host Configuration Protocol.

[83] LDAP - Liightghtwe Directory Access Protocol.

mecanismos de validação por autoridades acreditadas para o efeito. As aplicações usam ISCL para aceder ao sistema de distribuição e gestão de chaves (ex. *smart cards*).

As implementações em conformidade deverão adoptar um ou mais perfis de gestão de sistemas de segurança (Tabela 4), que poderão ser observadas em detalhe nos anexos de A a E do documento analisado [20], ao qual se segue uma descrição resumida.

Tabela 4 – Perfis de Gestão de Segurança

Perfil	Sub-Perfil	Descrição
Uso de Perfis de Segurança	-Online Electronic Storage Secure; -Basic Digital Signatures Secure; -Bit-Preserving Digital Signatures Secure.	Especifica o uso de perfis de segurança
Perfis de Segurança no Transporte e Conexão	-Basic TLS Secure Transport Connection -ISCL Secure Transport Connection -AES[84] TLS Secure Transport Connection	Descrição do protocolo e do mecanismo de negociação, da entidade de autenticação, dos mecanismos de encriptação e dos mecanismos de controlo de integridade que as implementações deverão suportar. No essencial os diferentes perfis diferenciam-se pelos mecanismos de segurança suportados e o nível de exigência de aplicação dos mesmos.
Perfil de Assinatura Digital (AD)	-Base RSA[85] Digital Signature -Creator RSA Digital Signature -Authorization RSA Digital Signature	Os perfis diferenciam-se pela forma como a assinatura digital é criada e pelo algoritmo de encriptação utilizado. O Supplement 86: Digital Signatures in Structures Reports, especifica orientações adicionais relativas à assinatura digital. Define o uso dos certificados X.509[86] e mecanismos apropriados de distribuição de chaves.
Perfil de *Media Storage Security*	-Basic DICOM Media Security	Especifica o encapsulamento de um ficheiro DICOM num ficheiro DIOCM seguro com as seguintes características de segurança: confidencialidade, integridade e autenticação da origem dos dados (opcional). Como algoritmo de encriptação, usa AES ou 3DES[87].
Perfil de Gestão do Endereçamento da Rede	-Basic Network Address Management	Especifica a utilização do DHCP para fornecer serviços de assinatura e gestão de IPs a máquinas remotas.
Perfil de Sincronização das Horas	-Basic Time Synchronization	Define serviços para sincronização de relógios de múltiplos computadores.
Perfil de Gestão da Configuração das Aplicações	-Application Configuration Management	Aplica-se aos serviços LDAP server LDAP client e DNS server.
Perfil Nível Básico de Confidencialidade das Aplicações	-Basic Application Level Confidentiality	Define um perfil básico com os seguintes aspectos: confidencialidade dos dados ao nível aplicação; confidencialidade nos outros níveis do modelo DICOM e integridade dos dados.

[84] AES – Advanced Encriptyon Standard.

[85] RSA - Rivest Shamir Adleman.

[86] X.509 - Digital Certificates.

[87] 3DES - Triple Data Encription Standard.

Em resumo, a norma DICOM diferencia-se dos outros formatos de imagens tais como JPEG[88], TIFF, GIF e outros por permitir que as informações dos pacientes sejam armazenadas, de forma estruturada, juntamente com a imagem, isto é, são armazenadas contendo etiquetas (*tags*) que identificam e delimitam as informações. A imagem propriamente dita na norma DICOM é baseada no formato JPEG com ou sem compressão, dependendo do equipamento que a gerou. Cada fabricante de equipamento de imagem pode implementá-la como quiser, desde que esteja em conformidade com a norma.

A vantagem desta estrutura é permitir fazer a leitura dos ficheiros e obter as informações necessárias, gerindo desta maneira as imagens e as informações dos pacientes de forma coerente e íntegra.

A norma DICOM é o maior projecto de normas de imagens médicas empreendido pela indústria, é uma norma complexa, mas não deixa de ser implementável e útil. A norma oferece uma estrutura modular sólida que assegura uma capacidade para desenvolver e responder a necessidades futuras. A quantidade de trabalho feito na DICOM tem sido a razão do interesse manifestado por outros especialistas.

A norma DICOM foi desenvolvida em conjunto com o Comité Europeu de Normalização (CEN TC 251) e com a JIRA (Japan Industries Association of Radiation Apparatus) e é analisada por organizações como o IEEE[89], HL7 e ANSI.

1.2 HL7

O grupo HL7 *(Health Level Seven)* é uma das organizações de desenvolvimento de normas [21], acreditada pela ANSI, que desenvolve padrões que, na maioria das vezes, são utilizados como especificações de mensagens, de forma a facilitar a comunicação de dados clínicos e administrativos entre sistemas de informação heterogéneos na área da saúde. Este grupo conta como participantes das iniciativas do HL7 países como a Suiça, Reino Unido, Finlândia, Holanda, Alemanha, China, Argentina, Austrália, entre outros.

Esta norma é amplamente usada nos EUA, mas o seu uso encontra-se também em expansão na UE. Este formato é imposto pela “Center for Medicare & Medicaid Services” (CMS) através do programa “Health Insurance Portability and Accountability Act of 1996” (HIPAA). Este programa tem como objectivo, entre outros, impor o uso de conjuntos de códigos e transacções nos sistemas de informação das entidades de saúde nos EUA.

É uma norma que genericamente se caracteriza da seguinte forma:

---

[88] JPEG - Joint Photographic Experts Group.

[89] IEEE - Institute of Electrical and Electronics Engineers.

- HL7 versão 3 é uma família de normas de comunicação orientada ao objecto, baseada no HL7 Reference Information Model (RIM);
- É aplicável em ambientes de rede e integra com o protocolo TCP/IP[90]. É baseado no modelo de referência OSI[91]. A norma HL7 situa-se ao nível das aplicações (nível 7);
- Especifica níveis de conformidade, descreve explicitamente como as entidades que a pretendam implementar devem proceder;
- As mensagens são estruturadas no formato XML.

O APEDEHE[92] é o protocolo HL7 mais utilizado. Este define as mensagens que são trocadas entre sistemas, sendo que as mensagens devem ser trocadas em ordem e código preestabelecidos.

A comunicação baseada na troca de mensagens HL7 suporta a integração funcional dos sistemas clínicos e administrativos, assegurando a automatização de processos.

Alguns exemplos de troca electrónica entre sistemas distintos são: a comunicação de dados, requisições e relatórios de e para laboratórios de Análises e de radiologia, receitas médicas, resumos de admissão e alta, Electronic Healthcare Record (EHR[93]) multimédia, informações sobre fármacos, etc.

A titulo de exemplo, uma mensagem HL7 que descreve o tipo de sangue de um dado doente: OBX|1|CE|ABOTYPE^ABO GROUP||OPOS^Type O|

A Microsoft criou uma solução que integra o HL7 com a sua ferramenta de integração e automação de negócios. O módulo de HL7 para Microsoft BizTalk descrito no seu site [22] aumenta as capacidades do BizTalk Server 2004 para empresas de assistência médica, ao fornecer uma solução HL7 de *messaging* que lhes permite partilhar informações sobre pacientes, tanto internamente como com outras entidades. Este componente do BizTalk para HL7 simplifica o processo de integração ao fornecer suporte pré-programado e detalhado para troca de mensagens HL7.

O grupo HL7 integra o Secure Transactions Special Interest Group (SIGSecure) endereçado para o desenvolvimento de transacções seguras HL7. Este grupo focaliza a sua atenção no uso do HL7 num ambiente de comunicações onde existe a necessidade de serviços de comunicações seguros como autenticação, encriptação, não repúdio e assinatura digital.

Para implementar transacções seguras HL7, este grupo baseia as suas ofertas no uso de mecanismos de segurança disponíveis e não propriamente em normalizar políticas de segurança.

---

[90] TCP/IP - Transmission Control Protocol/Internet Protocol.

[91] OSI - Open Systems Interconnection.

[92] APEDEHE - Application Protocol for Electronics Data Exchange in Healthcare Environments.

[93] EHR - Electronic Healthcare Record.

Genericamente, o SIGSecure identifica os requisitos do utilizador, os serviços necessários para conhecer esses requisitos, os mecanismos para fornecer esses serviços, e as especificações para implementar estes mecanismos.

No âmbito de actuação, este grupo limita-se ao fornecimento de mecanismos de segurança, ao nível da camada de aplicação, para transacções HL7 em rede e através da Internet, independentemente da camada de transporte.

O SIGSecure tem como meta explorar ao máximo as normas existentes, e publicitar especificações disponíveis. Adicionalmente, coopera com outros SDOs para evitar duplicação e promover a harmonização das normas.

A norma "Guide for EDI[94] (HL7) Communication Security" fornece uma estrutura de segurança para a comunicação electrónica de dados (EDI) ponto a ponto, baseada em mensagens HL7. É baseada num modelo comum de segurança e apresenta uma vista por diferentes níveis de grupos de utilizadores.

Este guia especifica os serviços internos de segurança necessários para fornecer segurança nas comunicações entre SIS[95]. Os serviços externos de segurança (como são os serviços fornecidos por uma Terceira Parte de Confiança (TTPs - Trust Third Parties)) destinam-se a facilitar as relações de confiança envolvidas nas comunicações.

Considerando os diferentes níveis de utilizadores, os mecanismos especificados e os detalhes da implementação, poderão ser usadas diferentes infra-estruturas de segurança (tais como chaves públicas ou infra-estruturas de chave simétrica) ou usar diversos protocolos de comunicação em diferentes níveis (tais como HTTP[96], SMTP[97] ou FTP[98]). Estas especificações de arquitectura aberta e flexível, permitem proteger os SIS das ameaças à segurança.

Com vista a proteger os SIS das ameaças à segurança (ex. *masquerading*, manipulação de dados, manipulação da origem dos dados, repúdio, etc.) e dos riscos a que estão expostas, alguns serviços de segurança oferecem autenticação e confidencialidade, enquanto que outros serviços tais como Integridade ou Autenticidade apenas proporcionam evidência de que um ataque ocorreu sem o prevenir tecnicamente. Os mecanismos de segurança podem ser implementados por: assinatura

[94] EDI - Electronic Data Interchange.

[95] SIS – Sistema de Informação para a Saúde.

[96]HTTP - Hyper Text Transfer Protocol.

[97] SMTP - Simple Mail Transfer Protocol.

[98] FTP - File Transfer Protocol.

digital, verificação do valor criptográfico, criptografia, auditora de segurança, etc.) de acordo com os diferentes níveis de segurança necessários, as diferentes políticas e aplicações.
Do ponto de vista da segurança do protocolo de comunicação, a aplicabilidade dos serviços de segurança não é específico de uma camada do modelo OSI, mas das várias camadas (Tabela 12).

Tabela 5 – Serviços de Segurança por Camada

Camada OSI	Mecanismos de Segurança
Ligação Lógica	L2TP[99], PPTP[100]
Rede	IPsec
Transporte	SOCKS[101], SSL[102], SSH[103], TLS
Aplicação	SHTTP[104], SFTP[105], PGP[106]/MIME[107], S/MIME[108], PKCS[109]#7

Uma arquitectura de rede cliente-servidor HL7 é composta por servidores de comunicação para comunicações ponto a ponto, onde as aplicações reúnem e trocam as suas mensagens. Os serviços de segurança HL7 fornecem comunicações seguras ao nível da camada de transporte ou de aplicação. Protecção adicional pode ser obtida usando a segurança dos serviços fornecidos ao nível das camadas de rede e de ligação.
Em comunicações seguras HL7, as mensagens HL7 são embrulhadas em envelopes seguros quando em trânsito (Figura 26). Estas podem ser arquivadas recorrendo a protocolos seguros de comunicação externos já implementados (SHTTP ou SFTP).

---

[99] L2TP - Layer 2 Tunnelling Protocol.

[100] PPTP - Point-to-Point Tunnelling Protocol.

[101] SOCKS - Sockets Secure Protocol.

[102] SSL - Secure Sockets Layer.

[103] SSH - Secure Shell.

[104] SHTTP - Secure HyperText Transfer Protocol.

[105] SFTP - Secure File Transfer Protocol.

[106] PGP - Pretty Good Privacy.

[107] MIME - Multipurpose Internet Mail Extension.

[108] S/MIME - Secure MIME.

[109] PKCS - Public Key Cryptography Standard.

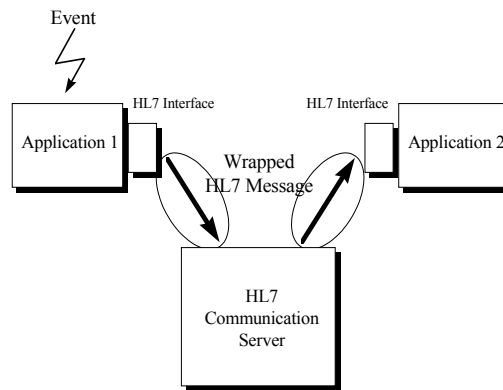



Figura 26 – HL7 Segurança nas comunicações

Para garantir a segurança das comunicações são usados protocolos como o IPv6, SSL e TLS, interfaces HL7 e LLP[110].

A interface HL7 existe ao nível da camada de aplicação do modelo OSI, mas por vezes também no servidor de comunicações. Esta situação requer suporte LLP (Lower Layer Protocol) que fornece interface entre HL7 e a rede. No sentido de obter ganhos de segurança, o uso deste mecanismo para transmissão de mensagens deverá ser assegurado pelos serviços de segurança definidos.

A norma "Guide for Implementing EDI (HL7) Communication Security" fornece detalhes que implementam segurança ponto a ponto EDI na comunicação HL7.

Para estabelecer comunicações seguras de mensagens EDI, requer a selecção e implementação de serviços apropriados de segurança como autenticação (utilizador, aplicação e sistemas), integridade, confidencialidade, e autenticidade no caso de não repúdio do emissor e/ou do receptor.

As recomendações baseiam-se na criptografia de chave pública com uma proposta de infra-estrutura de segurança forte PKI[111]. Para fortalecer a autenticação dos utilizadores é recomendado o uso de "*chipcards*" combinados com o código PIN e/ou sistemas biométricos.

O protocolo de comunicação mais indicado é o Secure File Transfer Protocol (SFTP).

Este protocolo de comunicação é baseado em TCP/IP e oferece aos utilizadores e sistemas autenticação, assim como, controlo e segurança na conexão. De acordo com a segurança das comunicações (Figura 26), SFTP embrulha mensagens HL7, selecciona e aplica vàrios métodos criptográficos tais como: PKCS#7, S/MIME, MOSS[112], PGP/MIME. Basicamente, o processo SFTP tem o seguinte funcionamento: o servidor está à escuta e tem o serviço FTP a correr no porto TCP 21, à espera de conexões cliente; antes de o cliente proceder à transferência de dados deverá existir autenticação forte entre as partes, de forma a assegurar a segurança na conexão.

---

[110] LLP - Lower Layer Protocol.

[111] PKI - Public Key Infraestruture.

[112] MOSS - MIME Object Security Services.

1.3 CEN/TC 251

O CEN *(European Committee for Normalization)* é a organização responsável pela criação de novas normas na União Europeia (EU) [23].

Na área da saúde foi criado um comité técnico denominado CEN/TC 251 – Medical Informatics, cujo objectivo é atingir compatibilidade, modularidade e interoperabilidade entre sistemas heterogéneos da saúde.

Estas normas incluem requisitos tais como procedimentos clínicos e administrativos, métodos e técnicas para suportar a interoperabilidade entre sistemas, qualidade e segurança.

O CEN/TC 251 é composto por 4 grupos de trabalho que cooperam entre si, sendo de realçar o trabalho desenvolvido pelo Working Group III (WGIII) – Security, Safety and Quality.

Este grupo de trabalho tem a cargo a gestão e desenvolvimento de normas de segurança e confidencialidade para a UE, e apresenta uma oferta consolidada no domínio dos SIS[113].

O desenvolvimento destas normas ocorre em paralelo com as normas básicas da informática para as comunicações nos SIS e os sistemas de registos electrónicos.

Algumas das normas desenvolvidos por este grupo podem ser observados na (Tabela 6), a referir por exemplo:

- ENV[114] 12924 – "Security Categorisation and Protection of Healthcare Information Systems";
- ENV 12388 – "Algorithm and Digital Signature Services in Healthcare";
- ENV 13608 – "Security for Healthcare Communication".
- O projecto SMIREC project – Secure Medical Record Information Communication [24].

Para garantir um reforço na segurança das comunicações, adicionalmente preconiza o recurso a cartões de identificação electrónicos, cartões profissionais de saúde, segurança nos cartões dos pacientes, assegurar *"timestamps"*, modelar políticas de segurança e qualidade nos SIS. As actividades relacionadas com os *"smartcards"* são relatadas e congregadas na *Task Force* "Intermittently Connected Devices". As actividades relacionadas com a segurança nas comunicações são relatadas na *Task Force* "Communication Security".

Esta organização opera a nível Europeu mas coopera com outros organismos relacionados com a normalização na área da saúde, por exemplo o ANSI-HISB, ASTM e HL7.

De seguida são apresentadas as principais normas desenvolvidas por este grupo de trabalho (Tabela 6).

---

[113] SIS – Sistema de Informação para a Saúde.

[114] ENV - European Pre-Standard.

Tabela 6 – Lista de normas de segurança CEN/CT 251 / WGIII

Abreviatura	Designação	Categoria	Descrição	Aspectos de Segurança	Mecanismos de Segurança
EN 13608 [1-3] 2005	Security for Healthcare Communication (SEC-COM).	Health Informatics Security	Define conceitos para a segurança de sistemas de saúde. Orientações para a segurança dos objectos de dados e do canal.	Segurança dos objectos de dados e do canal. Part 2 – Secure data objects; Part 3 – Secure data channels.	- Assinatura Digital; - Certificados Digitais; - Algoritmos de encriptação: TLS RSA, TLS SHA1-HMAC[115]; - Integrity Check Code; - Protocolo TLS.
ENV 12388 1996	Algorithm and Digital Signature Services in Healthcare.	Medical Informatics Security	Define algoritmo de assinatura digital para uso nos SIS na Europa. A norma baseia-se no algoritmo RSA.	Uso AD para: -autenticação utilizadores; -organizações e sistemas; -autenticação da origem dos documentos; -protecção da integridade dos documentos; -garantia de que conteúdo e assinatura são mantidos juntos;	- Assinatura Digital; - Selos Temporais; - Refere protocolos (ISO[116]/IEC[117] 9796, ISO/IEC 9798, ISO/IEC 13888)
EN 12251 2004	Secure User Identification for Healthcare – Management and security of authentication by passwords.	Health Informatics Security	Apresenta a gestão e segurança da autenticação por "senhas" nos SIS.	Autenticação individual dos utilizados por senhas.	Define politicas para gestão/segurança da identificação e autenticação dos utilizadores por senhas.
ENV 13729 2000	Secure User Identification for Healthcare. Strong Authentication using Microprocessor Cards.	Health Informatics	Orientada para a identificação segura dos utilizadores. Autenticação forte usando "chipcard".	Identificação segura dos utilizadores nos SIS.	-Cartões Profissionais de Saúde; -PIN e/ou identificação biométrica; -Certificados Digitais; -Protocolo cifrado; - TTP; -Proxy de autenticação; -Infra-estrutura de chave pública (X.509).

[115] SHA1-HMAC -

[116] ISO - International Standardization Organisation.

[117] IEC - International Engineering Consortium.

ENV 12924 1997	Security Categorization and Potection for Halthcare Iformation Systems.	Medical Informatics	Especifica um modelo, uma metodologia de categorização dos SIS baseado em segurança. Para cada categoria fixa e recomenda um conjunto de requisitos de protecção.	-Questionário de segurança; -Análise de risco; -Identificação de brechas de segurança.	Especifica mecanismos de protecção por categoria.
ENV 13606[1-3] 2000 EN 13606[4] 2005	Electronic Healthcare Record Communication (EHRcom).	Health Informatics	Orientações para a comunicação do registo electrónico do paciente.	Privilégios no acesso aos dados EHR. Part 4 – Security requirements and distribution rules.	-Autenticação das entidades; -Gestão de autorização, privilégios e controlo de acessos; -Integridade da informação EHR que é gravada, processada e comunicada; -Classificação de segurança da informação EHR; -Definição, negociação e ponte das políticas entre as entidades requerentes e fornecedoras de dados EHR; -Auditabilidade e rastreabilidade da informação acedida, processada e comunicada; -Total segurança e qualidade dos procedimentos. -Define politicas com base em: ISO/IEC 17799, EN 14484, EN 14485, ISO 22857 ISO/DTS 2260, ISO/TS 18308, RFC[118] 3881.
EN 14484 2003	International transfer of personal health data covered by the EU data protection directive - High Level Security Policy (HLSP).	Health Informatics	Directiva Europeia para a protecção de dados. A norma fornece um guia em HLSP que deverá ser adoptado por organizações envolvida em aplicações informáticas internacionais e na transmissão de dados de saúde a partir de um pais da EU para outros não pertencentes. Ex. Telemedicina e Teleconsulta.	HLSP na transferência de dados pessoais de saúde para um pais não membro da EU. Especifica princípios e artigos a adoptar na protecção de dados pessoais.	-Encriptação e assinatura digital durante a transmissão; -Prova de integridade e autenticação da origem; -Controlo de acesso e autenticação dos utilizadores, senhas com reforço por *"smartcards"*, sistemas biométricos e assinaturas digitais; -Necessidade de ambiente físico seguro; -Gestão da rede; -Controlo de vírus; -Relatórios de falhas/brechas de segurança; -Planos de contingência;

[118] RFC - Request For Comments.

					-Auditorias; -Medidas especiais de segurança.
EN 14485: 2003	Guidance for handling personal health data in international application in the context of the EU data protection directive.	Health Informatics	Guia para a protecção dos dados envolvidos em aplicações informáticas internacionais em que existe transmissão de dados pessoais de saúde entre países membros da EU e países não membros.	Especifica medidas a adoptar na protecção de dados pessoais de saúde nas transmissões entre países membros e não membros da EU.	-Medidas genéricas de segurança; -Contratos de segurança; -Políticas de segurança; -Análise de risco; -Segurança da organização e deveres; -Relatório de incidentes/brechas segurança; -Sensibilização do pessoal envolvido; -Transmissão em redes seguras; -Perfis de acesso aos dados; -Auditorias; -Planos de continuidade; etc.
CR 13694: 1999	Safety and Security Related Software Quality Standards for Healthcare (SSQS).	Health Informatics Security	Propostas de algumas normas de qualidade relacionadas com a segurança e protecção de software na área da saúde.	Referencia diferentes normas no âmbito da segurança.	Aspectos de segurança propostos pelas normas referenciadas nesta norma.
CR 14301: 2002	Framework for security protection of healthcare communication (SEC-COM/FR).	Health Informatics	O relatório descreve a estrutura de protecção de segurança na comunicação dos SIS.	Referencia outras normas no âmbito da segurança.	Aspectos de segurança propostos pelas normas referenciadas nesta norma.
CR 14302: 2002	Framework for Security Requirements for Intermittently Connected Devices (SEC-ICD).	Health Informatics	Define requisitos de segurança dos ICD assim como os cartões de pacientes que transportam informação clínica importante.	Planeamento básico para as normas Europeias dentro do mesmo assunto "Security Requirements for Intermittently Connected Devices".	Protecção da integridade dos dados, origem dos dados, autenticação, controlo de acesso e protecção da confidencialidade.

ENV 13608

A norma ENV 13608 (Security for Healthcare Communication (SEC-COM)) está orientada para a segurança dos objectos e do canal. As partes da norma relacionadas com os aspectos de segurança são:

A *Part 2 - Secure data objects,* define a forma de tornar os objectos de dados seguros. Define uma metodologia de segurança que permite que o objecto seja transportado de forma segura através de redes inseguras (independentemente do protocolo de transporte usado) ou armazenado em repositórios abertos e inseguros.

A aplicação é capaz de decidir qual a combinação de encriptação e assinatura digital (PKCS#7) a aplicar ao objecto. Algumas das soluções tecnológicas recomendadas ao nível da integridade e confidencialidade do objecto são o uso de mecanismos de "Integrity check code" e algoritmos de encriptação baseados em RSA e 3DES.

A *Part 3 - Secure data channels,* especifica serviços e métodos para tornar seguro comunicações entre SIS.

Define a segurança do canal e o protocolo de comunicação que implementam os seguintes serviços de segurança: autenticação das entidades antes de trocar dados, preservação da integridade dos dados e preservação da confidencialidade dos dados comunicados.

Especifica o uso do protocolo TLS junto com um perfil de encriptação, assim como um conjunto de soluções tecnológicas, de forma a garantir a integridade, confidencialidade e auditabilidade do objecto no canal. Sendo de realçar o uso de assinatura digital, certificados digitais (X.509) e algoritmos de encriptação do tipo TLS RSA e TLS SHA1-HMAC.

Esta norma é aplicável a múltiplos protocolos de comunicação usados nos SIS, incluindo DICOM, CORBA[119] (IIOP), HTTP, TELNET[120], POP3[121]/IMAP4[122] e outros.

ENV 12388

A norma (ENV 12388 - Algorithm and Digital Signature Services in Healthcare) define o algoritmo de assinatura digital para uso na UE pelos SIS. O algoritmo usado é RSA.

A assinatura digital é definida pelo ISO 7498, Part 2 – Gestão da Segurança das redes.

---

[119] CORBA - Common Object Request Broker Architecture.

[120] TELNET - Terminal emulation program for TCP/IP network.

[121] POP - Post Office Protocol.

[122] IMAP - Internet Message Access Protocol.

Referindo alguns exemplos de utilização da AD na autenticação de utilizadores, em organizações e sistemas, na autenticação da origem dos documentos, na protecção da integridade dos documentos, na garantia de que o conteúdo e a assinatura são mantidos juntos.

Alguns serviços de segurança adicional podem ser implementados junto com assinatura digital como por exemplo, não repúdio da origem e do receptor da mensagem, selo temporal, prova de autorização como profissional registado e outras qualificações.

O grupo ISO/IEC JTC1/SC27 trabalha nos protocolos. Este trabalho está dividido em mecanismos e técnicas, gestão de documentos suporte e linhas de segurança.

Na primeira categoria estão normas como:

- ISO/IEC 9796 - Digital Signature Scheme Giving Message Recovery;
- ISO/IEC 9798 - Entity Authentication; ISO/IEC 11770 Key Management;
- ISO/IEC 13888 - Non-Repudiation; ISO/IEC 14888 Digital Signatures with Appendix.

Na segunda categoria o SC27 é responsável por:

- ISO/IEC 13335 - Guidelines for the Management of IT Security;
- ISO/IEC 14516 - Guidelines for the Use and Management of Trusted Third Parties;
- ISO/IEC 15408 - Evaluation Criteria for IT Security.

EN 12251

A norma (EN 12251 - Secure User Identification for Healthcare – Management and security of authentication by passwords), orientada para a gestão e segurança da autenticação por senhas, foi projectada para melhorar a autenticação individual dos utilizadores dos SIS, fortalecendo a automatização dos procedimentos associados à gestão da identificação e senhas dos utilizadores, sem recorrer a facilidades ou hardware adicional (ex. smart cards ou sistemas biométricos).

A norma especifica um conjunto de requisitos referentes à gestão de utilizadores: Identificação e autenticação única; Identificação e autenticação antes de qualquer interacção; Associação de identificação única do utilizador; Manutenção da identidade dos utilizadores activos; Manutenção de logs; Não fornecer qualquer facilidade de partilhas de senhas; As senhas deverão ser armazenadas no sistema de forma cifrada; O sistema deve fornecer mecanismos de alteração da senha; Alteração de senhas de sistema por defeito; Temporização de validade de senhas; Complexidade da senha; etc.

ENV 13729

A norma (ENV 13729 - Secure User Identification for Healthcare - Strong Authentication using Microprocessor Cards (SEC-ID/CARDS)), orientada para a identificação segura do utilizador nos SIS. Autenticação forte através do uso de cartões profissionais de saúde e certificados digitais.

A norma define um modelo genérico de autenticação em que o utilizador está equipado com *chipcard* pessoal (neste contexto designado cartão profissional de saúde) e utiliza um protocolo cifrado. A Figura 27 descreve o processo de autenticação do utilizador.

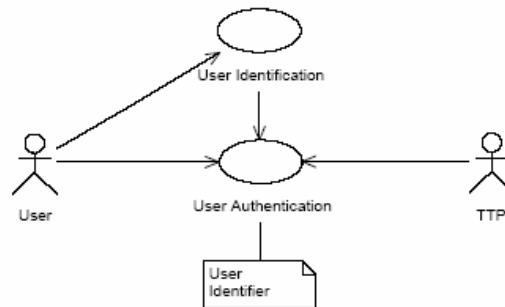



Figura 27 – Modelo de autenticação

No processo de autenticação é verificado o pedido de identificação do utilizador, baseado na informação de autenticação vinda do utilizador e de uma TTP (Trusted Third Party). O resultado é a verificação da identidade do utilizador. O cartão profissional contém a chave privada e o certificado digital do utilizador, fornecido por uma TTP. O cartão é inserido num terminal de cartões através do qual se realiza a autenticação. Como resultado do processo de autenticação, a identidade do utilizador é transferida para a aplicação médica.

A norma define os requisitos para o uso de cartões profissionais de saúde. Estes deverão estar conforme a norma ISO 7816 nos seguintes aspectos:

- Suportar o algoritmo de encriptação assimétrico RSA;
- Conter uma chave privada para autenticação;
- Protecção da chave através de PIN e/ou identificação biometrica;
- etc.

No sentido de fortalecer a autenticação especifica o uso de infra-estrutura de chave publica (X.509).

ENV 12924

A norma (ENV 12924 - Security Categorization and protection for healthcare information systems), fornece o significado do sistema por categorias baseado na resposta a questionário de segurança. Esta tarefa requer que seja realizada análise de risco ao sistema, assim como identificação de brechas de segurança. Este norma especifica os requisitos de protecção para cada categoria do sistema.

A norma específica um modelo e uma metodologia de categorização automática dos SIS no contexto da segurança e privacidade. Segurança é adquirida com significado de preservação, com um nível de aceitação de disponibilidade de dados, confidencialidade e integridade. Para este sistema

categorizado, corresponde um nível de requisitos de protecção e são fornecidas recomendações apropriadas ao nível de risco inerente a essa categoria.

ENV 13606

A norma (ENV 13606 - Electronic Healthcare Record Communication (EHRcom)) orientada para a comunicação do registo electrónico do paciente. Os aspecto se segurança são tratados na parte 4 da norma.

A *Part 4 - Security requirements and distribution rules*, da norma descreve uma metodologia e especifica os privilégios necessários para aceder a dados EHR[123]. Refere os requisitos gerais de segurança a aplicar em comunicações EHR, soluções técnicas e normas que especificam detalhes para satisfazer essas necessidades de segurança.

Em sistemas sensíveis como são os EHR, a informação tem que ser registada, armazenada, processada e comunicada em segurança.

Consequentemente a comunicação de EHR deverá reunir os seguintes requisitos de segurança:

- Autenticação das entidades (pessoas, software, dispositivos, etc.);
- Gestão de autorização, privilégios e controlo de acessos;
- Integridade da informação EHR que é gravada, processada e comunicada;
- Classificação de segurança da informação EHR;
- Definição, negociação e ponte das políticas entre as entidades requerentes e fornecedoras de dados EHR;
- Auditabilidade e rastreabilidade da informação acedida, processada e comunicada;
- Total segurança e qualidade dos procedimentos.

A norma refere um conjunto de requisitos de segurança para assegurar o acesso, comunicação e controlo de dados EHR:

Requisitos gerais de segurança com base na ISO/IEC 17799, que especifica formas de medir e a adoptar para proteger os dados EHR, e a forma como os dados podem ser comunicados em segurança como parte de um ambiente distribuído de computação.

Nas comunicações EHR fora EU, baseia-se em orientações e especificações de politicas de segurança nas normas EN 14484 e EN 14485. A ISO 22857 fornece informação similar quando um país não está incluído na EU.

Define uma arquitectura genérica para acesso e controlo de dados EHR.

---

[123] EHR - Electronic Healthcare Record.

O acesso a dados EHR é legitimado por um conjunto de políticas, algumas delas documentadas, outras codificadas dentro das aplicações e outras com autorização formal através de componentes do sistema. A norma ISO/DTS 2260 - Privilege Management and Access Control (PMAC[124]), define um modelo lógico genérico para representar os privilégios das principais entidades, o controlo das políticas de acesso e o processo de negociação que é requerido.
Requisitos de segurança específicos (como requisitos éticos e médico-legais) na comunicação de informação EHR, são expressos pela norma ISO/TS 18308.
Modelo genérico para políticas de acesso a EHR. É reconhecido de que a maioria dos sistemas clínicos e EHR incorporam medidas simples de controlo de acessos. A nova geração de sistemas permitem configurar políticas de acesso sofisticadas assim como o controlo das mesmas.
Auditorias detalhadas das interacções com os EHRs. Auditoria de interoperabilidade e comunicações a logs é feita com base no *draft* IETF[125] (RFC 3881).
O grupo de trabalho Europeu R&D no campo da segurança dos SIS está activamente a desenvolver especificações, e a definir perfis evolutivos de serviços de segurança. Muitos dos requisitos usados nas comunicações EHR são aplicáveis nas comunicações dos SIS em geral.

EN 14484

A norma (EN 14484 - International transfer of personal health data covered by the EU data protection directive - High Level Security Policy (HLSP)), fornece um guia em HLSP onde especifica um conjunto de aspectos restritivos e relevantes a adoptar por organizações, na transferência de dados de saúde pessoais de um pais membro da EU para um país não membro, nos casos em que o seu sistema de protecção de dados seja inadequado ao contexto desta directiva. A titulo de exemplo, aplicação da directiva na área Telemedicina e Teleconsulta.
Algumas das especificações e orientações emanadas pela directiva:

- Específica um conjunto de princípios e artigos a adoptar na protecção dos dados pessoais tais como: qualidade dos dados; critérios de legitimidade; processamento de dados pessoais especiais (raça, vida sexual, etnia, etc.) se satisfeitas condições especiais; direito no acesso aos dados; segurança no processamento; soluções judiciais, obrigações e sanções; autoridades supervisoras oficiais; transferência de dados pessoais para países terceiros; etc.

---

[124] PMAC - Privilege Management and Access Control.

[125] IETF - Internet Engineering Task Force.

- Fornece orientações no âmbito da transferência de dados pessoais, em formato electrónico ou em formato não electrónico (ex. papel, películas de radiografia, etc.), para países terceiros incluindo derrogações e cláusulas do contrato, bases em que a transferência para países terceiros é permitido (despersonalização dos dados, consentimento do paciente, exigência em termos de adequação da protecção dos dados, etc.).
- Fornece orientações constituídas por um conjunto de princípios, com ênfase para:
  - Principio 4 – segurança oficial na protecção dos dados;
  - Principio 5 – permissão para processar;
  - Principio 8 – proibição de transferência sem autorização do paciente;
  - Principio 10 – segurança no processamento;
  - Principio 12 – adequação do país terceiro na protecção dos dados.

No que se refere ao princípio 10, a directiva fornece linhas de orientação relativas à protecção dos dados de saúde contra a perda ou distribuição acidental, alteração ou acesso não autorizado.
Algumas das orientações estão relacionadas com:

- Análise de risco;
- Encriptação e assinatura digital durante a transmissão; prova de integridade e autenticação da origem;
- Controlo de acesso e autenticação dos utilizadores: recomenda o uso de senhas com reforços através de smart cards, sistemas biométricos e assinaturas digitais;
- Necessidade de ambiente físico seguro;
- Inclusão de aplicações de gestão e gestão da rede, a configuração da rede e gestão da firewall são aspectos vitais na segurança dos sistemas;
- Controlo de vírus; relatórios de falhas ou brechas de segurança; planos de contingência ou de continuidade do negocio em caso de falhas; auditorias;

Medidas especiais de segurança, no caso de os dados pessoais de saúde particularmente sensíveis (dados genéticos e dados relativos a doenças sexualmente transmissíveis), etc.

EN 14485

A norma (EN 14485 - Guidance for handling personal health data in international application in the context of the EU data protection directive), disponibiliza um guia para a protecção dos dados envolvidos em aplicações informáticas internacionais em que existe transmissão de dados pessoais de saúde entre países membros da EU e países não membros.

Com vista à protecção dos dados pessoais de saúde envolvidos nas transmissões, a norma propõe um conjunto de medidas de segurança: medidas genéricas de segurança; contratos de segurança com os processadores ou controladores dos países não membros; políticas de segurança; análise de risco; segurança da organização e deveres; relatório de incidentes de segurança e brechas; treino e sensibilização de todo o pessoal envolvido; transmissão dos dados em redes seguras; definição de perfis de acesso aos dados; auditorias, atitudes a tomar no caso de perda, dano ou destruição de dados; planos de continuidade em caso calamidade; etc.

CR 13694

A norma (CR 13694 - Safety and Security Related Software Quality Standards for Healthcare (SSQS)) apresenta uma visão de normas existentes ou emergentes que poderão ser aplicados aos SIS.

As normas consideradas são aqueles que focalizam a sua atenção na segurança do software, confidencialidade e integridade.

Este CR também examina normas no que se refere à sua aplicabilidade e adaptabilidade aos SIS, inclui organizações como: IEC, CEN, BSI[126], ASC X12, ASTM, CPRI e IEEE. Apresenta um sumário das normas que investigam os aspectos de segurança nos SIS.

Pela visão apresentada pelo CR, no futuro, as organizações que desenvolvem normas deverão dar grande importância aos aspectos de segurança do SIS. Especificamente as áreas que deverão ser endereçadas: determinação da criticidade nos SIS, definição das aproximações e métodos para desenvolvimento dos SIS, promoção de facilidades e testes de performance de sistemas clínicos e relatórios de operação dos mecanismos de monitorização.

CR 14301

O objectivo deste relatório (CR 14301 - Framework for Security Protection of Healthcare Communication (SEC-COM/FR)), é promover o entendimento das necessidades de segurança relacionada com as comunicações de informação de saúde. Esta norma referencia o uso das normas prEN 12805 e prEN 12806 [31].

CR 14302

O objectivo deste relatório (CR 14302 - Framework for Security Requirements for Intermittently Connected Devices (SEC-ICD)), é fornecer um planeamento básico para as normas Europeias dentro

[126] BSI - British Standards Institute, London.

do mesmo assunto "Security Requirements for Intermittently Connected Devices" [32]. É um guia para o grupo de trabalho CEN TC224/WG12 que prepara normas específicas para implementar mecanismos de segurança, e requisitos a usar por equipamentos de leitura de cartões de saúde.

No campo de aplicação este guia serve para outros projectos que use cartões de saúde para os pacientes, profissionais e outras pessoas ligadas ao sector dentro da Europa.

Este relatório define requisitos de segurança para os sistemas "intermittently connected devices" e discute requisitos para os seguintes serviços de segurança: Protecção da integridade dos dados, origem dos dados, autenticação, controlo de acesso e protecção da confidencialidade.

O relatório define requisitos de segurança para as interfaces dos ICD entre aplicações e o sistema ICD. Em particular define o acesso a diferentes tipos de dados ICD, restrito a diferentes classes de pessoas (profissionais, outras.) ou ao paciente. Direitos de leitura, alteração e remoção de dados.

Em resumo o committee CEN TC 251 encontra-se a trabalhar na área dos "Health Informatics" e "Medical Informatics" sobre algumas funções de segurança e serviços como: CR - Framework for Formal Modelling of Healthcare Security Policies; ENV - Accountability and Audit Trail Mechanism for Healthcare Information Systems; ENV - Access Control Policy Bridging; ENV - Risk Assessment Procedures; ENV - Data Protection Contract Guidance.

1.4 ISO/TC 215

A ISO (International Organization for Standardization) [25] é uma organização mundial, que prepara normas internacionais elaboradas por um conjunto de comités técnicos. O ISO TC 215 é um comité técnico criado especialmente para a área da informática médica. O âmbito deste comité técnico é a normalização no campo da informação para a saúde e a normalização das tecnologias das comunicações necessárias para atingir a compatibilidade e interoperabilidade entre sistemas independentes.

A ISO TC 215 "*Health Informatics*" teve início no mesmo âmbito que o CEN TC 251. Ambos os comités têm colaborado no mesmo sentido, já que os seus objectivos quase que se sobrepõem. O trabalho da ISO tem-se focado em aspectos básicos da informática médica.

A ISO TC 215 é composto por vàrios grupos de trabalho, sendo de realçar o trabalho desenvolvido pelo Working Group 4 (WG 4) – Security.

Este grupo de trabalho tem a seu cargo a definição de normas para contra medidas técnicas, de modo a assegurar confidencialidade, disponibilidade, integridade e responsabilidade, bem como os princípios gerais para a administração da segurança na área da saúde. Aqui, não se introduzem novas tecnologias específicas da área da saúde, mas procuram-se definir perfis de normas de segurança entre sectores, que sustentam os requisitos necessários para esta área.

Algumas das normas desenvolvidos por este grupo podem ser observados na (Tabela 7), a realçar:

- ISO/TS 17090 – "Public Key Infrastructure"
- ISO/WD 27799 – "Security management in health using ISO/IEC 17799"

A Tabela 7 lista algumas das normas relacionadas com a segurança, no domínio "Health Informatics" [26] [27].

Tabela 7 – Lista de normas de segurança ISO/TC 215 / WG4

Abreviatura	Designação	Categoria	Descrição
ISO/TS 17090 2002	Public Key Infrastructure	Health Informatics	Descrição sobre a utilização de PKI no domínio da informática Médica.
ISO 22857 2004	Guidelines on data protection to facilitate trans-border flows of personal health information	Health Informatics	Guia para protecção de dados que deverá ser aplicado na transferência internacional de informação pessoal de saúde.
ISO/WD 27799 2005	Security management in health using ISO/IEC 17799	Health Informatics	Proporciona um guia que suporta a interpretação, implementação e acompanhamento da norma ISO/IEC 17799 na área da saúde.
ISO/TS 18308 2004	Requirements for an electronic health record architecture (EHRarchitecture)	Health Informatics	O seu propósito é fixar os requisitos clínicos e técnicos para uma arquitectura de registos electrónicos de saúde, que suporte o uso, a partilha e intercâmbio dos registos clínicos electrónicos entre diferentes sectores da saúde e diferentes países.
ISO/TS 21091 2005	Directory services for security, communications and identification of professionals and patients.	Health Informatics	Define as especificações mínimas para um directório de serviços para a área da saúde usando a estrutura X.500. Esta especificação técnica fornece um directório comum de informação e serviços necessários para suportar a segurança nas transacções de informação de saúde através de redes públicas.
ISO 21549 2004	Patient Healthcare Data	Health Informatics	Define um modelo básico orientado ao objecto para os cartões de saúde. Define uma estrutura para armazenamento dos dados clínicos do paciente.
ISO/TR 16056 2004	Interoperability of telehealth systems and networks.	Health Informatics	Orientada para a interoperabilidade das redes e sistemas de telemedicina.
ISO/TC 22600	Privilege Management and Access Control.	Health Informatics	Define um modelo para a gestão de privilégios e controlo de acessos.

ISO/TS 17090

A norma (ISO/TS 17090 – Public Key Infrastruture), oferece uma descrição sobre a utilização de PKI no domínio da informática médica.

O comité responsável IST/35 - Health Informatics, através do draft ISO 17090 oferece uma descrição da norma, decomposta em três partes:

A Parte 1 - Overview of Digital Certificate Services [27], define os conceitos básicos subjacentes ao uso da assinatura digital nos SIS, fornece um esquema e identifica os serviços de segurança necessários para a comunicação segura de informação de saúde, quando os certificados digitais são requeridos. Faz um resumo dos componentes básicos necessários para desenvolver uma assinatura digital e apresenta cenários para utilização de certificados digitais no SIS, como pode ser observado na Tabela 8.

Tabela 8 – Cenários e serviços nos SIS

Service	Scenario number															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Authentication	X		X	X	X	X	X	X	X	X	X	X	X	X	X	
Confidentiality	X		X			X	X	X	X	X	X		X			
Integrity		X		X	X		X	X						X		
Digital signature		X		X	X			X			X	X	X	X	X	X

Key to scenarios

1 ER access to records
2 Temporary services (emergency aid)
3 Enroll new member
4 Tele imaging
5 Automated results reporting
6 Results reporting/Practitioner messaging
7 Patient physician treatment discussion
8 Patient care registry summary
9 Patient pharmacist question
10 Patient pharmacist messaging
11 Remote access to clinical info system
12 Emergency access
13 Remote transcription
14 Electronic transcription
15 Autenticate physician order
16 Potential uses of digital signatures in healthcare

Para cada um dos cenários faz uma descrição da forma como é feito o acesso à informação clínico do paciente, com e sem o recurso a assinaturas digitais. No caso do não recurso à assinatura digital, é necessário que os documentos sejam impressos e assinados pela pessoa autorizada e enviados em suporte papel (por exemplo: Análises, Exames clínicos, Relatórios clínicos, etc.) para a entidade responsável pelo tratamento.

Através do uso de certificados digitais, no acesso à informação clínica do paciente, é possível verificar a identidade e credenciais do emissor do documento.

A Parte 2 - Certificate Profile [28], para a área da saúde fornece perfis específicos de certificados digitais baseados na norma X.509 versão 3. Para diferentes tipos de certificados, os perfis estão baseados na especificação IETF/RFC 3280 e IETF/RFC 3039. A norma especifica os “Certificate

Profile" requeridos, para o intercâmbio de informação de saúde dentro de uma organização, entre diferentes organizações, e através países com jurisdição diferente.
A Parte 3 - Policy Management of Certification Authorit [29], oferece linhas de orientação para a gestão de certificados digitais na área da saúde. Define uma estrutura e os requisitos mínimos para a política de certificados, assim como as praticas associadas. Relativamente às políticas de segurança na área da saúde, e além fronteiras, identifica as principais necessidades em termos de comunicações e define o nível mínimo de segurança permitido. Na base da especificação está o IETF/RFC 3647.

ISO / TS 22857

A norma (ISO/TS 22857 – Guidelines on data protection to facilitate trans-border flows of personal health information), providencia um guia na protecção de dados que deverá ser aplicado na transferência internacional de informação pessoal de saúde.
Define um conjunto de regras e princípios relativos à importação e exportação de dados, os controladores e os processadores, que uma organização deverá adoptar para estar em conformidade.
Preconiza uma política de segurança elevada: recurso à encriptação e assinatura digital na transmissão e importação de dados; controlo de acessos e autenticação; auditorias; segurança física; gestão da infra-estrutura da rede; antivírus; planos de contingência; detecção de falhas de segurança, etc.
O uso desta norma serve para facilitar a transferência de dados pessoais de saúde internacionalmente e garantir aos pacientes de que os seus dados são adequadamente protegidos quando enviados para, e processados noutro país. Esta norma deverá ser usado por hospitais, indústria farmacêutica, fornecedores de serviços médicos remotos, bases de dados ou bancos de registos médicos com pacientes de diferentes países assim como organizações envolvidas internacionalmente por exemplo no e-commerce e no e-pharmacy.

ISO / TS 27799

A norma (ISO/WD 27799 – Security Management in Health Using ISO/IEC 17799) proporciona um guia para as organizações prestadoras de cuidados de saúde, e outros detentores de informação de saúde na implementação da norma ISO/IEC 17799, com o propósito da confidencialidade, integridade e disponibilidade da informação pessoal de saúde.
Define um plano de acção para implementar a norma ISO/IEC 17799 providenciando uma cheklist de controlo em 11 áreas contendo um total de 39 categorias de segurança. Esta norma tem sido amplamente adoptada pela Austrália, Canada, Netherlands, New Zealand, South Africa e United Kingdom, na gestão da segurança dos SIS.

Todos os objectivos de controlo descritos pela norma ISO/IEC 17799 são relevantes na área da Informática Médica, mas alguns dos controlos requerem uma explicação adicional na forma de usar para proteger a confidencialidade, integridade e disponibilidade da informação de saúde. Existe também alguns requisitos adicionais específicos do sector da saúde.

ISO / TS 18308

O propósito da norma (ISO/TS 18308 - Requirements for an Electronic Health Record Architecture) é fixar os requisitos clínicos e técnicos para uma arquitectura de registos electrónicos de saúde, que suporte o uso, a partilha e intercâmbio dos registos clínicos electrónicos através de diferentes sectores relacionados com os cuidados de saúde, diferentes países, e diferentes modelos transferência de informação clínica.

ISO / TS 21091

A norma (ISO/TS 21091 - Directory services for security, communications and identification of professionals and patients), define as especificações mínimas para um directório de serviços para a área da saúde tendo por suporte uma infra-estrutura de chave pública. Endereça um directório na área da saúde numa perspectiva comunitária em antecipação ao suporte inter-empresas, inter-jurisdição e comunicações internacionais na área dos cuidados de saúde.

A norma também suporta um directório de serviços com apontadores que suportam a identificação de profissionais de saúde, organizações e pacientes / consumidores. Por último inclui nos serviços alguns aspectos relacionados com os índices mestres de pacientes.

O directório da área da saúde apenas suporta o standard LDAP.

ISO / DIS[127] 21549

A norma (ISO/DIS 21549: 2004 – Patient Healthcare Data), define um modelo básico orientado ao objecto para os cartões de saúde (Figura 28 – Cartão de Saúde do Paciente), é uma estrutura flexível, e foi desenhada para facilitar o armazenamento dos dados clínicos do paciente.

É constituída por varias partes, e define a estrutura geral dos dados para diferentes tipos de cartões de saúde transportados pelos pacientes. A ISO/IEC 7810 especifica a estrutura dos cartões ao longo de 5 partes. São elas: *Part 1- General Structure; Part 2- Common Objects; Part 3- Limited Clinical Data; Part 4 – Extended Clinical Data; Part 5 – Identification Data; Part 6 – Administrative Data; Part 7 – Electronic Prescription.*

---

[127] DIS - Draft International Standard.

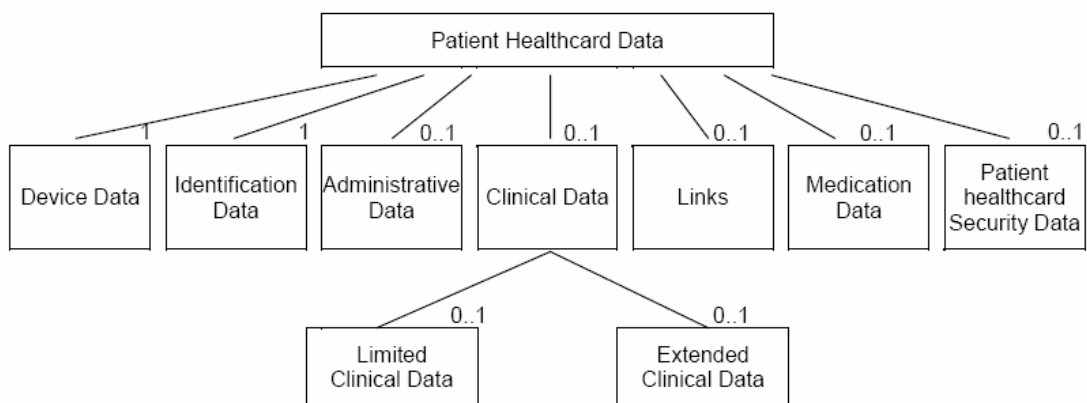



Figura 28 – Cartão de Saúde do Paciente

O acesso remoto às bases de dados de saúde e aos sistemas de suporte, deverá ser por pessoal autorizado com autenticação através de dispositivos que implementem funções de segurança, assim como o uso de assinaturas digitais.

Os dados relacionados com o cartão estão categorizados e três tipos: Identificação, dados administrativos e dados clínicos. Nesta categorização também está incluído o item "Patient Healthcare Security Data".

O cartão de dados do paciente deverá oferecer algumas facilidades tais como: transmitir informação clínica de um agente prestador de cuidados de saúde a outro agente, fornecer índices e/ou autorizações para aceder a informação clínica relacionada com o cartão do utente.

A norma providencia uma série de atributos de segurança, como pode ser observado no documento "DRAFT INTERNATIONAL STANDARD ISO/DIS 21549", no *ponto – Device and Data Security Attributes,* definidos na Part 2 – Common Objects [54]. A norma fornece uma série de funções de segurança apropriadas, como por exemplo: o atributo *direito de acesso*, este direito pode ser controlado por um sistema automático, i.e. o uso de cartões profissionais de saúde; o atributo *serviços de segurança*, necessário para o armazenamento dos dados, requer mecanismos de segurança. Os serviços de segurança associados aos dados do cartão do paciente são deverão contemplar autenticação; o acesso a dados de saúde associados ao cartão do paciente deverá ser mediante funções de identificação, controlo de acesso e assinatura.

ISO / TR 16056

Esta norma (ISO/TR 16056 - Interoperability of Telehealth Systems and Networks) está orientada para a interoperabilidade dos sistemas de telemedicina e redes.

A *Part 1 - Introduction and definitions*, apresenta uma breve introdução à interoperabilidade dos sistemas de Telemedicina e redes. No anexo informativo descreve os vários componentes da telemedicina.
A *Part 2 - Real-time systems,* define o campo de aplicação da norma relacionado com aplicações em tempo real (incluindo vídeo, áudio e conferencia de dados), define requisitos de interoperabilidade no âmbito dos sistemas de Telemedicina e redes, identifica e constrói blocos para tornar as soluções interoperaveis.
Este documento endereça quatro áreas específicas: Standards for real-time telehealth systems; Interoperability issues in telehealth applications; Requirements for interoperable telehealth systems and networks; e Framework for interoperable architectures.
Esta norma é usada por organizações ou fornecedores que implementem soluções de Telemedicina.

ISO / TC 22600

A norma (ISO/TC 22600 - Privilege Management and Access Control), define um modelo para a gestão de privilégios e controlo de acessos. Estes privilégios são baseados nas normas ISO e CEN. Referencia o uso da norma ISO/TS 17090 – Public Key Infrastruture e o DTS – Directory Services for Comunications and Identification of Professional and Patient. A norma divide-se em três partes:
A Part 1 – Overview and Policy Management, descreve os cenários e os parâmetros críticos no intercâmbio da informação. Dá exemplos da documentação necessária.
A Part 2 – Formal Models, descreve e explica em detalhe a arquitectura e o modelo de privilégios, gestão de privilégios necessário para partilha de informação segura.
A Part 3 – Implementations, descreve a aplicação de serviços de segurança. Autenticação, integridade, confidencialidade, disponibilidade, serviço de notariado, controlo de acesso e auditabilidade são aspectos analisados e descritos no modelo conceptual.

1.5 OMG

CORBA (Common Object Request Broker Architecture) é uma tecnologia *midleware* que foi definida pela OMG (Object Management Group) [31]. CORBA é uma tecnologia orientada ao objecto que torna possível o desenvolvimento escalável e reutilizável de software que seja independente da plataforma de software e do sistema operativo. Um objecto CORBA representa-se por um interface que possui um conjunto de métodos.
A OMG criou dois grupos de trabalho, CORBAmed e CORBA Security Service (CORBAsec) que cooperam entre si no sentido de promover a segurança necessária nos sistemas de saúde.
O CORBAmed [32] é designado por Domain Task Force na área da informática médica. Define as tecnologias para a interoperabilidade dos sistemas, i.e., define interfaces normas orientadas ao

objecto entre sistemas de saúde de forma a promover a interoperabilidade entre diferentes plataformas, linguagens e aplicações.

Algumas das actividades mais importantes do CORBAmed estão representadas na Figura 29.

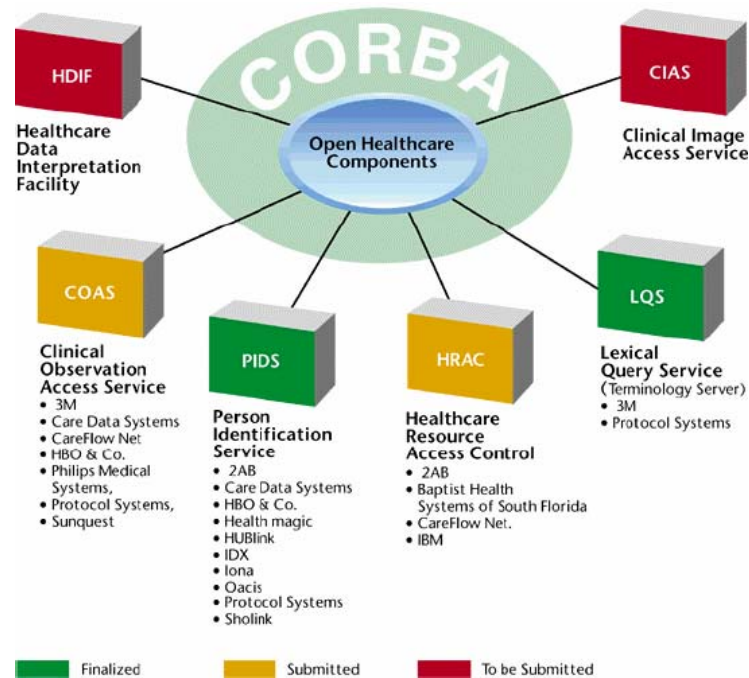



Figura 29 – Serviços disponibilizados pelo CORBAmed

O CORBAsec centra a sua actividade na área da segurança, desenvolvendo funcionalidades de segurança tais como: identificação e autenticação, delegação de privilégios, autorização e controlo de acesso, auditoria de segurança, não repúdio, confidencialidade e encriptação, integridade da informação, segurança nas comunicações entre objectos, disponibilidade, domínios de segurança e gestão de politicas de segurança. Um *overview* detalhado sobre especificações dos serviços de segurança poderá ser encontrado em [33].

A Figura 30 apresenta o modelo para objectos CORBA-Security. A todos os objectos invocados são aplicadas funções apropriadas de segurança de forma a fortalecer as politicas de segurança assim como o controlo de acesso.

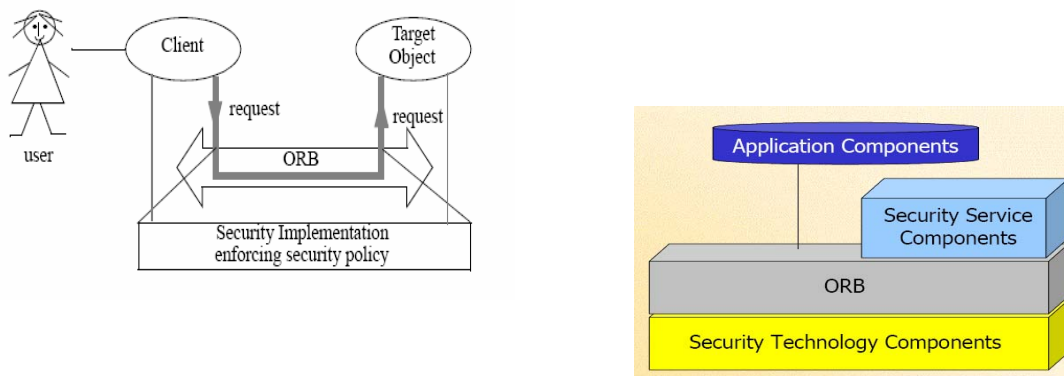



Figura 30 – Modelo Segurança Objectos CORBA

O CORBAsec possui um conjunto de especificações disponíveis [34]: Authorization Token Layer Aquisition Service (ATLAS); Common Secure Interoperability, Version 2 (CSIv2); CORBA Security Service (CORBAservices); Public Key Interface (PKI); Resource Access Decision (RAD); Security Service Protocol (SECP).

As especificações ATLAS e RAD fornecem funcionalidades de segurança ao nível do API[128]. CSIv2 e CORBA *Security Services* fornecem melhorias em termos de segurança à infra-estrutura CORBA.

As abordagens que melhor atendem às necessidades deste ambiente devem estar baseadas num modelo de confiança, com base numa infra-estrutura de chaves públicas, cujo objectivo é facilitar o desenvolvimento de sistemas computacionais distribuídos escaláveis e seguros.

1.6 HIPPA

O HIPAA (Health Insurance Portability na Accountability Act) [35] estabelece um padrão constituído por um conjunto de regras a seguir na troca de informações de eventos de saúde pelas entidades envolvidas. O HIPAA foi efectivado em Abril de 2003 e instituído nos EUA, é uma determinação legal para as instituições de saúde.

Este padrão preconiza implementar políticas e procedimentos que garantam a privacidade da informação em formato electrónico e dos sistemas. Simplificadamente os requisitos do HIPAA envolvem cinco elementos [38] [39]: transacções electrónicas codificadas; segurança; identificação única; assinatura electrónica; e privacidade.

Em alguns pontos do HIPPA existe interacção paciente/hospital [36] [37], por exemplo para permitir acesso ao paciente aceder aos seus registos e corrigir eventuais erros o paciente deverá ser informado da forma como a sua informação pessoal é usada. Outro aspecto envolve questões como a confidencialidade da informação do paciente e a existência de procedimentos documentados de

---

[128] API - Application Programming Interface.

privacidade [40]. Estes pontos carecem de regulação específica, a referir: *Update* de *software*; consultadoria especializada; alguns casos reestruturação do edifício médico; e sistemas de registos.

1.7 IEEE

O principal objectivo do IEEE (Institute of Electrical and Electronics Engineers) [41] é cooperar no avanço global promovendo o processo de engenharia na criação, desenvolvimento, integração, partilha e aplicação de conhecimento sobre tecnologias de electricidade. O principal trabalho desta instituição na criação de normas para aplicação na área da saúde tem sido desenvolvido através dos grupos MEDIX e MIB, como podemos ver na Tabela 9.

Tabela 9 – Lista de grupos IEEE

Abreviatura	Designação	Descrição
IEEE P1157	Medical Data Interchange - MEDIX	Norma de troca de informação entre Sistemas Informáticos Hospitalares
IEEE P1073	Medical Information Bus (MIB)	Desenvolver meios de comunicação entre aparelhos de cuidados intensivos e computadores

Actualmente, este instituto não possui nenhum grupo activo na área da segurança e confidencialidade. O grupo IEEE/MEDIX coopera com outras organizações no desenvolvimento de normas na área da segurança.

1.8 EDIFACT

A segurança para mensagens EDIFACT (Electronic Data Interchange For Administration, Commerce and Transport) [42], através do grupo de trabalho em segurança UN/EDIFACT, partilhado com Terry Dosdale de United Kingdom, iniciaram a construção da versão 4 do EDIFACT com a sintaxe ISO 9735. Na Europa, o Western European EDIFACT Board (WE/EB) coordena as actividades de 10 grupos responsáveis pelo desenho de mensagens para diferentes campos de aplicação inclusive, na área médica.

Suportam o desenvolvimento de projectos, nomeadamente “TEDIS projects” (Data interchange and the information services), “ENVI_D_I Project” (Environmental Data Interchange).

A norma “ISO 9735 - Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT) - Application level syntax rules”, define uma metodologia de construção de mensagens EDI que contêm dados seguros ou encriptados. Os algoritmos usados são: DES, IDEA, RSA, RIPEMD-160, etc. Utiliza esquemas de assinatura digital.

As partes da norma que tratam as questões de segurança são:

A Part 5 - Security rules for batch EDI (Authenticity; integrity and non-repudiation of the origin) - especifíca a sintaxe e regras de segurança EDIFACT. Fornece um método para endereçar níveis de mensagens/pacotes, nível de segurança no intercâmbio de mensagens, autenticação, integridade e não repúdio da origem das mensagens, em concordância com os mecanismos de segurança.

A Part 6 - Secure authentication and acknowledgement message (Message type – autack) - define a segurança, autenticação e reconhecimento de mensagens AUTACK (AUThentication and ACKnowledgement).

A Part 7 - Security rules for batch EDI (confidentiality) - endereça níveis de mensagens/pacote, níveis de segurança para o intercâmbio de mensagens, níveis de segurança para a confidencialidade, em concordância com os mecanismos de segurança estabelecidos.

A Part 9 - Security key and certificate management message (message type - KEYMAN) - define as regras para chaves de segurança e a gestão de certificados.

A Part 10 - Security rules for interactive EDI - especifica regras e a sintaxe para intercâmbio seguro de mensagens EDI. Fornece um método para endereçar níveis de intercâmbio para a segurança de mensagens / pacotes, de acordo com os mecanismos de segurança estabelecidos.

1.9 ASTM

A ASTM (American Society for Testing and Material) [43] através do comité E31 em sistemas computorizados estabeleceu a divisão em segurança e confidencialidade em 1996, cujo objectivo era acelerar o desenvolvimento de normas de segurança e confidencialidade no âmbito SIS (Tabela 10), e coordenar normas de segurança desenvolvidos por outros SDOs.

Tabela 10 – Sub -Comités ASTM

Sub -comité	Descrição	Objectivo
E31.17	Privacy, Confidentiality, and Access.	Desenvolver normas relacionadas com os aspectos de segurança, acesso, privacidade e confidencialidade dos registos de pacientes
E31.20	Data and System Security for Health Information.	Definir o processo de autenticação nos SIS e trabalhar em colaboração com outras organizações nestes aspectos

O trabalho destes sub -comités centra-se nos aspectos de segurança dos SIS, sendo de realçar algumas normas desenvolvidas:

- E1762-95: 2003, Standard Guide for Authentication of Healthcare Information;
- E2084, Standard Specification for Authentication of Healthcare Information Using Digital Signatures. Authentication and Authorisation to Access Healthcare Information, Internet and Intranet Security for Healthcare Information;
- Secure Timestamps for Healthcare Information;

- Data Security, Reliability, Integrity and Availability for Healthcare Information;
- Distributed Authentication and Authorisation to Access Healthcare Information.
- E1869, Standard Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information including Computer Based Patient Records;
- Documentation of access for Individually-Identifiable Health information;
- Standard Guide for Confidentiality and Security Training of Persons Who Have Access to Health Information;
- Standard Guide for Amendments/Additions to Health Information by Healthcare Providers, Administrative Personnel, and by the Subjects of Health Information;
- Standard Guide to the Transfer/Disclosure of Health Information in an Emergency Treatment Event;
- Standard Guide for the Use and Disclosure of Health Information;
- Policy Guide for the Transfer/Re-disclosure of Health Information Between Health Plans;
- Guide for Rights of the Individual in Health Information;
- Standard Guide to the Use of Audit Trials, and for Access and Disclosure Logging/Tracking in the Management of Health Information;
- Security and Confidentiality of Dictated and Transcribed Health Information.
- E2212-02[a], Standard Practice for Healthcare Certificate Policy - endereça politicas para os certificados digitais, estes suportam autenticação, autorização, confidencialidade, integridade e requisitos de não repúdio de pessoas e organizações que electronicamente criam e transaccionam informação de saúde.

No documento ASTM Draft Standard (ISO/TC 215/WG4 / N86: 2001), é descrita a arquitectura para directoria, certificação e registo de serviços fornecidos no âmbito dos SIS. Esta arquitectura está orientada para o fornecimento de uma directoria de elementos necessários para tornar segura a troca de informação de saúde através de redes públicas, recorrendo ao uso de uma infra-estrutura PKI.

1.10 CPRI

O CRPI (Computer-based Patient Record Institute) [44] desenvolve normas de segurança na área dos registos médicos. Através do grupo de trabalho em confidencialidade, privacidade e segurança, sobre a co-orientação de Kathleen Frawley, JD e Dale Miller, desenvolverão orientações no âmbito do contrato de confidencialidade, requisitos de segurança, glossário de termos de segurança e listas de trabalho para sistemas de segurança.

Algumas orientações disponíveis:

- Guidelines for Establishing Information Security Policies;
- Guidelines for Information Security Education Programs;
- Guidelines for Managing an Information Security Program;
- Security Features for CPR Systems;
- Sample Confidentiality Statements and Agreements;
- An Overview of Healthcare Information Standards;
- Guidelines for Electronic Signature Policies;
- Healthcare Security Related Projects within the Telematics Applications Program of the European Commission.

1.11 ISO/IEC 17799

A norma ISO/IEC 17799: 2005 – Code of Practice for Information Security Management (Gestão da Segurança da Informação).

Em 1987 o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (Commercial Computer Security Centre) que dentro das suas atribuições tinha a tarefa de criar uma norma de segurança das informações para o Reino Unido.

Desde 1989 vàrios documentos preliminares foram publicados por esse centro, até que, em 1995, surgiu a BS7799 (British Standard 7799). Esse documento foi disponibilizado em duas partes para consulta pública, a primeira em 1995 e a segunda em 1998. A *Part 1 - Code of Practice for Information Security Management,* e a *Part 2 - Specification for Information Security Management Systems.*

Em Dezembro de 2000, após incorporar diversas sugestões e alterações, a BS7799 ganhou *status* internacional com a sua publicação na forma de ISO/IEC 17799:2000 - Code of Practice for Information Security Management [45] [46], a qual possui uma versão aplicada aos países de língua portuguesa, denominada NBR ISO/IEC 17799 [48].

A "norma ISSO/IEC 17799 – Gestão da segurança da informação" pode ser definida como a protecção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno dos investimentos e as oportunidades de negócio.

A ISO17799 cobre os mais diversos tópicos da área de segurança, possuindo um grande número de pontos de controlo e requisitos a ter em consideração para garantir a segurança da informação de uma organização (Tabela 11), de forma que a obtenção da certificação pode ser um processo demorado e muito trabalhoso.

Em contrapartida, a certificação é uma forma bastante clara de mostrar à sociedade que a organização dá a importância merecida à segurança da sua informação e à dos seus clientes, de tal forma que se prevê que em poucos anos as grandes organizações terão aderido à norma e obtido suas certificações.

Tabela 11 – Itens referidos pela norma ISO/IEC 17799: 2000

Itens	**Objectivo**
Política de Segurança	Definir uma política de segurança, e publica-la e comunicá-la através de toda a organização.
Segurança organizacional	Promover uma infra-estrutura de segurança da informação na organização.
Classificação e controle dos activos da informação	Manter a protecção adequada dos activos de informação.
Segurança nas pessoas	Reduzir os riscos de erro humano, roubo, fraude ou uso indevido de instalações.
Segurança física e do ambiente	Prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização.
Gestão das operações e comunicações	Garantir a operação segura e correcta dos recursos de processamento da informação.
Controlo de acesso	Controlar o acesso à informação.
Desenvolvimento e manutenção de sistemas	Garantir que a segurança seja parte integrante dos sistemas de informação.
Gestão da continuidade do negócio	Não permitir a interrupção das actividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.
Conformidade com requisitos	Garantir conformidade dos sistemas com as leis, estatutos, regulamentações, obrigações contratuais, políticas e normas organizacionais de segurança e de quaisquer requisitos de segurança.

Através do trabalho realizado pelo comité técnico ISO/ IEC JTC 1/ SC27 – IT Securities Techniques, em Junho de 2005 assistimos à publicação da nova versão da ISO/IEC 17799: 2005. A revisão deste referencial de excelência no que concerne a segurança da informação traz diversas novidades [49] [50], não só à forma como está organizado, mas também a nível conceptual, alterações estas que se traduziram na inclusão de um novo capítulo e em cerca de 17 novos controlos e na fusão ou remoção de controlos antigos presentes na versão de 2000, perfazendo agora um total de 134 controlos distintos que as organizações devem analisar e implementar consoante as suas necessidades e requisitos de negócio.

O novo capítulo de controlos que podemos encontrar na ISO/IEC 17799:2005 encontra-se subordinado à problemática da Gestão de Incidentes de Segurança da Informação (Information Security Incident Management) e inclui o estabelecido no quarto capítulo da versão de 2000, Segurança dos Elementos Humanos (Personnel Security) ao nível da resposta a incidentes de segurança. A inclusão de um capítulo que se debruça sobre a necessidade de monitorização, detecção, investigação, recolha de evidências e resposta a incidentes e falhas de segurança de informação, é uma adição bem recebida, uma vez que um dos princípios intrínsecos à ISO/IEC 17799 e à BS7799-2 (actual ISO/IEC 27001) é precisamente a aprendizagem e melhoria contínua do ISMS (Information Security Management System - Sistema de Gestão de Segurança da Informação) por parte das organizações.

Alguns dos capítulos da ex. -ISO/IEC 17799:2000 foram renomeados e sofreram alterações significativas; com especial atenção para os capítulos: Organizing Information Security (Organização da Segurança da Informação) que diferencia as relações ou responsabilidades do nível de segurança da informação, por parte de colaboradores internos e por parte de entidades externas; Asset Management (Gestão de Recursos) que inclui actualmente a necessidade de definição do uso aceitável dos recursos organizacionais, por parte dos seus colaboradores; e Human Resources Management (Gestão de Recursos Humanos), agora dividido em três sub-capítulos que incidem sobre os controlos de segurança da informação cuja implementação é aconselhável antes, durante e após o vínculo laboral entre o colaborador e a organização, uma alteração necessária atendendo à relevância que as pessoas têm para o alcance da segurança da informação nas organizações, mas também às ameaças que podem representar e trazer para a confidencialidade, integridade e disponibilidade da informação crítica de negócio das organizações.

No sentido de melhorar a sua usabilidade, a revisão e reorganização da ISO/IEC 17799, deixou marcas na estrutura do referencial não apenas ao nível conceptual mas também ao nível do conteúdo. É esperado que em 2007 a ISO/IEC 17799:2005 passe a ISO/IEC 27002, inserida na nova série ISO/IEC 2700x.

Diversos programas de software estão disponíveis no mercado para ajudar a implementar o padrão BS 7799 / ISO 17799 e a desenvolver politicas de segurança. Callio Secura 17799 é um deles [47]. Traz consigo uma metodologia completa, questionários, um guia de informação, e todas a ferramentas necessárias para se desenvolver um sistema de gestão de segurança da informação e acelerar a sua implementação.

1.12 ISO 7498

A ISO 7498: 1988, descreve um modelo básico de referência para interconexão de sistemas abertos (*OSI – Open System Interconnection*). O objectivo do OSI é permitir a interconexão de sistemas heterogéneos.

A *parte 2 - Security Architectur*, da norma providencia uma descrição genérica dos serviços de segurança e mecanismos, e também define a posição relativa ao modelo onde os serviços e mecanismos são fornecidos. Esta parte estende o campo de aplicação da norma de forma a cobrir comunicações seguras entre sistemas abertos.

Esta norma define cinco categorias principais de serviços de segurança (Tabela 12):

Tabela 12 – Serviços de Segurança segundo a norma ISO 7498

Categoria	Objectivo	Mecanismos	Observações
Autenticação	Assegurar que no momento em que o serviço estiver a ser	Controlo de vulnerabilidades; Métodos de autenticação;	Controlo senhas. CEN/TC 12251

	utilizado, uma entidade é realmente quem diz ser.	Controlo de acessos.	
Controlo de Acessos	Controlar o acesso aos dados protegidos.	Protecção contra acessos não permitidos.	Regras de controlo de acessos. CEN/TC 12251
Integridade dos dados	Protecção dos dados contra alterações não autorizadas. Remoção, inclusão, ou modificação de dados.	Métodos de validação e correcção dos dados; Codificações; Assinaturas Digitais.	ENV 12388
Confidencialidade	Protecção de informação registada para que apenas pessoas autorizadas possam ter acesso.	Legislação; Normas; Protecção de dados.	CNPD – Comissão Nacional Protecção de dados. Funções de controlo e fiscalização do processamento de dados pessoais.
Não Repúdio	Impedir o repúdio ou a possibilidade de rejeição da origem da informação.	A origem tem que fornecer meios que permitam ao receptor provar a origem da informação.	

1.13 ISO / IEC 13335

O propósito desta norma é fornecer um guia para a gestão dos aspectos de segurança das Tecnologias de Informação *(Guidelines for Management of IT Security)*.

Esta norma é constituída por três partes: A *Part 1 – Concepts and models for IT Security, e*sta parte do relatório fornece orientações básicas para um responsável pela gestão da segurança numa organização. A *Part 2 – Managing and planning IT Security,* esta parte descreve a forma de gestão e planeamento dos aspectos de segurança. Esta descrição cobre os seguintes itens: políticas de segurança das TI, organização dos aspectos de segurança das TI, gestão de riscos, implementação e seguimento e a *Part 3 – Techniques for the management of IT Security,* descreve as técnicas de segurança apropriadas a usar durante o ciclo de vida do projecto, como planeamento, desenho, implementação, teste, aquisição e operação.

1.14 SEGNAC 4

O SEGNAC 4 - Normas para a Segurança Nacional, Salvaguarda e Defesa Matérias Classificadas, Segurança Informática.

Resolução do Conselho de Ministros n.º 5/90, de 28 de Fevereiro, que aprova as instruções sobre a segurança informática [51].

As instruções emanadas pela resolução definem princípios básicos, normas e procedimentos destinados a garantir a segurança e protecção das matérias classificadas no âmbito dos organismos do Estado, quando transmitidas por meios eléctricos e electrónicos.

Algumas das instruções relativas:

- Segurança física das instalações (áreas de segurança, estrutura das instalações, energia eléctrica, climatização, protecção contra incêndios e radiações electromagnéticas, controlo de entradas e saídas, etc.);
- Segurança de suportes físicos (controlo de circulação, caracterização de suportes magnéticos e ópticos, protecção contra radiações, etc.);
- Segurança Lógica (controlo lógico de acessos, controlo dos dados, manutenção, etc.);
- Classificação, preparação e segurança de dados e programas classificados;
- Reprodução, transferência, controlo de segurança e destruição de dados e programas classificados.

A revisão e as propostas de alteração às normas competem à Comissão Técnica do Sistema de Informações da República Portuguesa, em coordenação com a Autoridade Nacional de Segurança.

1.15 H.323

O H.323 é uma recomendação da International Telecommunications Union (ITU[129]) que estabelece os padrões para comunicações multimédia sobre redes de comutação de pacotes, como são as LANs, MANSs, WANs e a Internet. O protocolo H.323 fornece uma base para as comunicações de dados, áudio e vídeo de redes baseadas em IP, incluindo a Internet. Por atender o protocolo H.323, os dados multimédia e aplicações de diversos fornecedores podem operar, permitindo a comunicação entre utilizadores sem preocupações quanto a compatibilidade.

As recomendações H.323 focam dois tipos de sessões multimédia: ponto-a-ponto e multiponto. No caso da teleconsulta é usado uma sessão ponto-a-ponto; sessão multiponto é usada no caso de teledidáctica.

Para os sistemas de videoconferência usados em telemedicina, uma implicação é que uma sessão seja segura.

O relatório "*United Kingdom Research and Education Networking Association*" [52], descreve as recomendações de segurança referentes ao padrão H.323, conclui-se que a criptografia ao nível de aplicação do H.323 está no início, e portanto, a criptografia só pode ser garantida ao nível da camada de rede, por exemplo, através do uso de VPNs ou IPsec.

As redes sem fios suportam uma variedade de opções para videoconferência por intermediar distâncias entre espaços sem fio e com fio. Os componentes tipicamente exigidos incluem equipamento de videoconferência conectado a um dispositivo com capacidade para operar num rede sem fios que transmite para um ponto de acesso conectado a uma rede com fios [53].

---

[129] ITU - International Telecommunication Union.

As redes sem fios locais estão a tornar-se comuns nas instituições de saúde, e então a pergunta que se coloca é se a videoconferência pode ser feita através destas redes. A resposta é, sim. A dificuldade em implementar a videoconferência é que o vídeo e áudio exigem mais qualidade de rede do que outro tipo de tráfego (por exemplo, o envio de um e-mail ou navegação na rede). A perda de pacotes e a competição de tráfego na rede sem fios poderão causar falhas no vídeo e no áudio. Outro factor desfavorável ao vídeo e áudio sobre redes sem fios, é que redes sem fios são totalmente partilhadas por todos os utilizadores, de modo que os utilizadores competem pela mesma largura de banda e a qualidade do vídeo e voz degrada-se mais rápido.

A maior atracção da videoconferência via satélite é a sua flexibilidade. Todo equipamento necessário para esta tecnologia é completamente transportável e pode ir aonde for necessário. Mas esta tecnologia de comunicação sofre dos mesmos efeitos que o vídeo em redes sem fios e alguns mais. A latência é inerentemente maior devido ao atraso da velocidade da luz para e do satélite. Porém, a maioria dos utilizadores pode ajustar rapidamente e superar os problemas do atraso. Outro problema é que as taxas de transmissão de dados do satélite podem ser diferentes para *Uplink* e para *Downlink*, fazendo com que a videoconferência simétrica se torne mais difícil.

2 Sistemas de Classificação e Codificação

Os sistemas de classificação e codificação clínica são aqui referidos, pela sua importância no contexto da normalização do vocabulário médico. A classificação e codificação da informação clínica estão directamente relacionadas com a integridade dos dados clínicos.

O **ICD** (International Classification of Diseases) [69], foi criado pela Organização Mundial de Saúde, com vista a codificar e classificar informações médicas, criando um padrão para definir causa "mortis" em atestados de óbito. A Classificação Internacional de Doenças é revista de 10 em 10 anos, os códigos estão agora na sua 10ª revisão (ICD-10), no entanto muitos países incluindo Portugal ainda usam o ICD-9. Para codificar uma determinada condição do doente é necessário navegar por um extenso sistema de classificação de diagnósticos ou procedimentos.

Os **DRG** (Diagnosis Related Groups) ou **GDH** (Grupo de Diagnóstico Homogéneos) [70] são um sistema de classificação de episódios de internamento. Foram criados na Universidade de Yale nos anos 80 com a finalidade de constituir um sistema de pagamento prospectivo (SPP), tendo vindo a ser rotineiramente utilizados pelo Medicare (sistema de saúde americano) desde 1986. Os DRG derivam de uma extensão do ICD e são usados para facilitar o reembolso e a análise de casos do tipo "case−mix" [71]. Estes grupos não têm a especificidade clínica para terem valor nos cuidados médicos de um doente ou na investigação clínica. Em Portugal são usados desde 1989. Os objectivos são: classificar dados de morbilidade e mortalidade, com propósito estatístico; indexar arquivos hospitalares por doenças e procedimentos; armazenar os dados e o seu tratamento estatístico para pesquisas.

O **UMLS** (Unified Medical Language System) da National Library of Medicine (NLM) [72], tem como objectivo facilitar o desenvolvimento de sistemas computorizados que se possam comportar como se entendessem o significado da linguagem biomédica e da saúde. Para esse fim, a NLM produziu e distribuiu a base de conhecimento UMLS e programas informáticos associados para serem usados por criadores de sistemas na construção de sistemas de informação electrónicos que criem, processem, recuperem, integrem e/ou agreguem dados e informação biomédica. A base de conhecimento UMLS tem múltiplos fins. Ela não está optimizada para uma aplicação em particular, mas pode ser aplicada em sistemas que realizem um número funções envolvendo um ou mais tipos de informação, tais como, registo de pacientes, literatura científica ou dados de saúde pública.

O **SNOMED** (Standard Nomenclature of Medicine) é uma nomenclatura criada para indexar o conjunto de registos médicos, incluindo sinais, sintomas, diagnósticos e procedimentos [73] [74]. Esta norma é aceite para descrever o resultado de testes patológicos.

Um diagnóstico na SNOMED consiste num código topográfico, num código morfológico, num código de organismo vivo e num código funcional.

Esta norma, está a ser usada em Portugal, pela especialidade de Anatomia Patológica por exemplo.

A **CIPE** (Classificação Internacional para a Prática de Enfermagem) um tipo de classificação que permite a implementação de novos sistemas de informação e documentação em enfermagem. Começa a generalizar-se nas organizações e serviços a nível nacional [75]. Esta realidade prende-se com a necessidade de representar formalmente o conhecimento de enfermagem, usando uma linguagem comum que permita a produção de informação acerca das decisões e dos resultados da prática da enfermagem. Para tal é necessário usar uma linguagem classificada, sendo a CIPE [76] a que se revela mais adequada. Em alguns contextos onde foi implementada, tem-se revelado uma ferramenta fundamental, porque permite adequar o diagnóstico à concepção de cuidados de enfermagem, planear intervenções baseadas em evidência, utilizar planos de cuidados verticais, permitindo a percepção da condição problemática do utente/família e percepcionar os resultados obtidos face à evolução do diagnóstico.

Da Análise da documentação de enfermagem que se desenvolve nos serviços que estão a implementar novos sistemas de informação, tem sido possível perceber a ausência de coerência dos dados de enfermagem com a situação diagnóstico do doente, situando-se estes apenas na descrição das actividades desenvolvidas na prática clínica. Logo, tudo o que favoreça a produção de informação relacionada com a situação do doente é relevante e oportuno.

Para além dos sistemas de classificação e codificação referidos, importa ainda salientar a tecnologia **XML**[130] que oferece aos utilizadores a possibilidade de criar documentos com dados clínicos organizados de forma hierárquica de uma forma simples e estruturada.

---

[130] XML – Extensible Markup Language. Para mais informação ver RFC 3076.

Anexo B – Componentes de uma Arquitectura de Infra-estruturas de Chaves Pública

O núcleo de uma infra-estrutura PKI *(Public Key Infrastructure)* baseia-se em quatro serviços de segurança: registo, certificação, chave e directório, que incluem um conjunto de componentes acessórios sendo de realçar a recuperação de chaves, o sistema cruzado de certificados e o serviço de selos temporais.

Os elementos que compõem esta estrutura caracterizam-se por um conjunto de funções específicas que, interligadas, permitem realizar o objectivo da PKI [3]. São eles:

2.1 Registo e Certificação

As *Autoridades de Registo* ("Registration Authority" (AR)) são responsáveis por guardar e verificar toda a informação que a CA precisa para emitir o certificado. Em particular a CA deve verificar a identidade do utilizador para iniciar a emissão do certificado no CA. Esta é uma operação "física" que exige, por exemplo, a apresentação de um cartão de identidade, estando em geral próximo dos utilizadores.

As principais funções da RA são: verificar a identidade e as declarações do requerente; manipular o certificado do requerente; validar a identidade de um indivíduo, entidade, ou servidor. Uma RA não pode emitir certificados, apenas pode agir como intermediária.

A *Autoridade Certificadora* ("Certification Authority" (CA)) é a entidade respondível pela emissão e administração dos certificados digitais. O CA actua como sendo o agente de confiança na PKI. As suas funções são: gerar ou fornecer os meios técnicos necessários para a geração dos pares de chaves e emitir certificados digitais; emissão de chaves para os utilizadores; certificação das chaves públicas dos utilizadores; publicação dos certificados dos utilizadores; responsável pela revogação de certificados e pela publicação da Lista de Certificados Revogados ("Certificate Revogation List" (CRLs[131])).

As suas principais tarefas são: a recepção dos pedidos de certificação e de revogação feitos pela AR; gerar o certificado baseado numa chave pública.

Tipicamente gera um par de chaves (a chave privada é guardada num "smart card" ou "token USB"); garante a existência de um único par de chaves e faz a ligação entre um certificado e um utilizador em particular; gere os certificados publicados. Faz parte de um sistema cruzado de

[131] CRL - Lista de Certificados Revogados.

certificação com outros CAs, em que assina certificados de outras CAs. Assim publica num repositório público, toda a informação de revogação de certificados. Assina e arquiva na sua base de dados, todos os dados históricos *"Logs"*. De referir que a "Root CA" que se encontra no topo da hierarquia, gera o seu próprio par de chaves.

2.2 Serviços Acessórios

Serviço de Directório: tem duas funções principais: publicação de certificados; publicação da lista de revogação de certificados ou publicação "online" do "status" de um certificado. O sistema universalmente aceite é o directório X.500, em que as aplicações têm acesso aos certificados por LDAP (Lightweight Directory Access Protocol).

Serviço de Revogação de Certificados: é necessário por vários motivos: as chaves podem ficar comprometidas, por existirem colaboradores que abandonam as organizações, ou como medida administrativa para retirar o acesso a colaboradores a informação de uma forma temporária ou definitiva. Os certificados revogados são tipicamente referenciados numa CRL. As CRL's podem ser publicadas num directório público (X.500). A grande questão é fazer a verificação da CRL sempre que é utilizado um certificado. Esta operação pode ser realizada manualmente, o que é trabalhoso e que facilmente os utilizadores deixam de fazer, ou nem sequer se apercebem da sua necessidade. Idealmente, esta operação deve ser realizada automaticamente pelo software de cliente.

Sistema de Recuperação e Cópia de segurança de Chaves: é uma necessidade óbvia em ambientes institucionais, porque deve ser possível recuperar informação cifrada em determinadas circunstâncias, por exemplo, quando os utilizadores perdem as suas chaves, abandonam a organização, esquecem-se da senha de protecção das chaves, ou as chaves são destruídas ("smart card", discos, disquetes, etc.)

Sistema de Gestão de Chaves e Certificados: as caves e certificados devem ser periodicamente renovadas para incrementar a segurança, e devem ser actualizadas antes de expirarem, caso contrário haverá uma interrupção de serviço. A actualização pode ser realizada manual ou automaticamente. A actualização manual apresenta várias dificuldades para os utilizadores. Esta actualização deverá ser o mais transparente para o utilizador e realizada de forma a não interromper o serviço.

Serviço de Suporte ao não repúdio: ninguém deve poder repudiar um documento com assinatura digital. Para isso a chave de assinatura deve estar na posse do utilizador (sem cópia de segurança central) e bem guardada. O modelo mais comum é o do (um) par de chaves, que no entanto apresenta os seguintes problemas: se as chaves são geradas no ambiente de trabalho e guardadas de forma segura, há suporte ao não repúdio, mas não hà cópias de segurança (problema de

cópias de segurança e recuperação de chaves). Se forem geradas centralmente e arquivadas para evitar o problema anterior, não hà suporte ao não repúdio. Desta forma, temos um conflito entre não repúdio e cópia de segurança de chaves!

Uma solução possível é a utilização de dois pares de chaves (Dual Key Pair), em que hà: chave privada de assinatura + chave pública de verificação; chave pública de cifra + chave privada para decifrar. O par de chaves de assinatura é gerado localmente. A chave de assinatura deve ser bem guardada. O par de chaves de cifra é gerado e guardado centralmente e guardados (backup de chaves).

Outra solução é proteger no servidor o certificado com uma "passfrase" que o utilizador deve memorizar e que não deve ficar registado pelo sistema. Em termos de segurança é uma solução de compromisso entre segurança e praticabilidade.

Serviço de Mobilidade: os utilizadores devem poder usar as suas chaves em locais diferentes, o que coloca a questão da mobilidade. Algumas soluções passam pelo uso de "smart cards", "USB token" ou soluções de "roaming".

Certificação Cruzada: a "confiança" centralizada numa dada CA não é compatível com a natureza humana nem com os modelos organizacionais. Há, portanto necessidade de manter o controlo sobre em quem se confia e ter a flexibilidade de incluir ou excluir organizações. A certificação cruzada estende os relacionamentos de confiança TTP (Third Party Trust) entre domínios de autoridade de certificação.

Gestão de Políticas: a definição escrita das políticas a aplicar às CAs, RAs e aos utilizadores é considerada de fundamental importância. Este documento deverá reger todas as regras para a gestão e utilização de certificados e assinaturas digitais. São estas regras que permitem uniformizar o sistema e geram confiança no mesmo.

Actualização Automática das Chaves: um certificado deve ter um prazo de validade e ser automaticamente substituído por outro antes do prazo expirar. Idealmente, não haverá qualquer intervenção por parte do utilizador. Sempre que o certificado está a ser utilizado o seu prazo de validade é verificado. Sempre que a data de expiração está próxima, ocorre uma operação de renovação e um novo certificado é gerado. Então o novo certificado passa a ser utilizado em substituição do anterior.

Gestão do Historial de Chaves: o software deve ter mecanismos para aceder ao histórico de chaves para, de forma transparente para os utilizadores, decifrar dados com chaves antigas.

Serviço de Selos Temporais e Notariado (Timestamping): todas as máquinas tem que estar na mesma área temporal (horas). Este é um serviço especial que confirma a recepção de documentos digitais numa data específica.

É, portanto, um processo que associa uma data/hora a um documento. O utilizador submete o "hash" do documento ao sistema de "Timestamping" e o sistema devolve o "hash" do documento juntamente com a data/hora digitalmente assinado.

Software do Cliente: há dois aspectos que valorizam uma PKI: as funcionalidades que a PKI disponibiliza e a possibilidade de aplicações e equipamentos utilizarem criptografia e certificados. O software do cliente deve estar preparado para reconhecer, originar e reagir a todos os eventos inerentes. Deve requerer os serviços de certificação e de revogação, deverá compreender os historiais das chaves e saber quando requerer uma actualização ou recuperação de chaves, etc.

Entre as aplicações tipo que podem fazer uso de uma PKI, encontram-se: o correio electrónico; o ambiente de trabalho (segurança ficheiros/pastas); os browsers (clientes e servidores); VPNs.

Anexo C – Grelha de Avaliação dos Aspectos de Segurança num Sistema de Informação Clínica

C1 – Classes de Aspectos a Avaliar

Aspectos a Avaliar	Autenticidade	Confidencialidade	Integridade	Disponibilidade	Outros
Auditabilidade	+				
Autenticação do utilizador	+				
Prevenção, detecção e recuperação de intrusões	-	+	+	+	
Disponibilidade do sistema				+	
Resistência a corrupção de dados			+		
Tolerância a falhas		-	-	+	
Conformidade com normas			+		+
Documentação para administração e utilização					+
Comunicações					
Interrupção das comunicações				+	
Escuta das comunicações		+			
Personificação nas comunicações			+		
Repetição de comunicações			+		
Risco físico			+		
Cifragem		+			
Escalabilidade					
Pontos críticos	+	+	+	+	
Poder do Administrador		+	+		
Resistência a perda de confidencialidade		+			
Flexibilidade para reconfiguração					
Especificação de procedimentos de administração (conveniencia/facilidade)	+	+	+	+	
Especificação de procedimentos de utilização (conveniencia/facilidade)	+	+	+	+	

C2 – Grelha de Classificação dos Sistemas de Informação Clínica

Avaliação dos aspectos de segurança (exemplos de questões)							Legenda: 1-Fraco; 2-Insuficiente; 3-Razoável; 4- Bom; NA-Não Aplicável; NS-Não Sei
Aspectos a Avaliar	**Avaliação**						**Justificação**
	1	**2**	**3**	**4**	**NA**	**NS**	
Autenticação e Autorização dos utilizadores							
São utilizados mecanismos de autenticação por tipo de utilizador (administrador, utilizador, gestor, etc)? Quais são?							
Existem políticas de senhas? São alteradas regularmente?							
São dadas e controladas as permissões por tipo de utilizador?							
Confidencialidade dos dados							
Existem mecanismos de garantia de confidencialidade no acesso aos dados em operação normal?							
E em situação de ataque? Os mecanismos de protecção são suficientemente robustos?							
E no caso de acesso aos dados para estudos estatísticos ou científicos?							
Integridade dos dados							
Existem mecanismos que permitam controlar a integridade dos dados em operação normal?							
E em situação de ataque? Os mecanismos de protecção são suficientemente robustos?							
Existe procedimentos de verificação, correcção e controlo de qualidade dos dados?							
Disponibilidade do sistema							
Existem mecanismos para garantir a disponibilidade do sistema em operação normal?							
Existe mecanismos para contrariar potenciais ataques ao sistema do tipo "Negação de Serviços"?							
Tolerância a falhas do sistema em caso de avaria? E em caso de ataque?							
Existência de pontos críticos informáticos?							
Existência de pontos críticos físicos?							

Auditabilidade							
Existe registos que permitam efectuar auditoria?							
Que informação é registada?							
Existe verificação regular desses registos?							
Que meios suportam esses registos?							
Utilização ao nível de administração							
A administração do sistema é remota ou tem de ser feita na consola?							
Quais os mecanismos de autenticação utilizados? Existem cuidados especiais?							
De que forma é feita a protecção da sessão de administração remota?							
Os procedimentos de administração estão documentados?							
As interfaces são fáceis de perceber e utilizar?							
Em situação de elevada carga do sistema o administrador têm prioridade de acesso?							
É possível configurar o sistema de diferentes formas, para diferentes utilizadores?							
Que poderes tem o administrador? Existe diferentes tipos de administradores?							
Acessos ao sistema para estatística?							
Utilização normal							
O acesso ao sistema é remoto ou local?							
A utilização do sistema está devidamente documentada?							
Mecanismos de autenticação utilizados?							
As interfaces são fáceis de perceber e utilizar?							
Em situação de elevada carga do sistema?							
Acessos ao sistema para estatística?							
Conformidade a normas							
O sistema está em conformidade com certificações oficiais?							
Qual é o grau de conformidade?							

Mecanismos de defesa							
É usado algum sistema criptógrafico de protecção?							
A que nível são usados os mecanismos criptográficos? (Ao nível aplicação, ao nível do sistema ou ao nível da rede?)							
Grau de robustez do sistema criptográfico? (Qual o algoritmo e o comprimento das chaves de cifra?)							
Existe mecanismos para prevenção de intrusão?							
Existe mecanismos para detecção de intrusão?							
Existe mecanismos de recuperação em situação de intrusão?							
Comunicações							
Tipos e meios de comunicação usados?							
Os meios usados são propícios a escuta?							
Existe mecanismo para garantir a integridade da informação em trânsito?							
Existe mecanismo de certificação do utilizador de forma a prevenir o "disfarce"? Qual?							
Existe mecanismo para prevenir a interrupção das comunicações?							
Documentação							
Existe informação técnica para administração do sistema?							
Existe informação para a utilização do sistema?							